

Modules

Jasper Ty

What is this?

These are notes I am taking about the theory of modules, while taking Jonah Blasiak's Abstract Algebra I class at Drexel.

The content is being taken mostly from Nathan Jacobson's *Basic Algebra I*, Chapter 3, although the class is using Dummit and Foote.

Contents

I	Modules over a principal ideal domain	I
1.1	The ring of endomorphisms of an abelian group	1
1.2	Left and right modules	7
1.3	Fundamental concepts and results	8

I Modules over a principal ideal domain

I.1 The ring of endomorphisms of an abelian group

We extend the story of groups arising from considering composition of maps.

Definition 1.1.1. The **ring of endomorphisms** $\text{End } M$ of an abelian group $(M, +)$ is the set of all homomorphisms $M \rightarrow M$, with ring structure given by

$$(\eta\zeta)(x) := \eta(\zeta(x)), \quad (\eta + \zeta)(x) := \eta(x) + \zeta(x)$$

for all $\eta, \zeta \in \text{End } M$ and $x \in M$. From this definition, it follows that 1 is the map $x \mapsto x$ and 0 is the map $x \mapsto 0$.

Paperwork ahead!

■ **Theorem 1.1.2.** $\text{End } M$ is a ring.

Proof. First we prove that M 's addition is an abelian group.

Every statement in this proof holds for all $A, B, C \in \text{End } M$:

1. **ADDITION IS CLOSED.**

In other words, the pointwise sum of two abelian group homomorphisms is again an abelian group homomorphism.

For all $x, y \in M$,

$$\begin{aligned} (A + B)(x + y) &= A(x + y) + B(x + y) \\ &= (A(x) + A(y)) + (B(x) + B(y)) \\ &= A(x) + B(x) + A(y) + B(y) \\ &= (A + B)(x) + (A + B)(y), \end{aligned}$$

so $A + B \in \text{End } M$.

2. **ADDITION IS ASSOCIATIVE.**

For all $x \in M$,

$$\begin{aligned} (A + (B + C))(x) &= A(x) + (B + C)(x) \\ &= A(x) + (B(x) + C(x)) \\ &= (A(x) + B(x)) + C(x) \\ &= (A + B)(x) + C(x) \\ &= ((A + B) + C)(x). \end{aligned}$$

So $A + (B + C) = (A + B) + C$.

3. **THE ZERO MAP IS THE UNIT OF ADDITION.**

Let $\bar{0}$ denote the map $x \mapsto 0$. Then $\bar{0}$ is an abelian group homomorphism, as

$$\bar{0}(x + y) = 0 = 0 + 0 = \bar{0}(x) + \bar{0}(y)$$

for all $x, y \in M$.

For all $x \in M$,

$$(A + \bar{0})(x) = A(x) + \bar{0}(x)$$

$$\begin{aligned}
&= A(x) + 0 \\
&= A(x).
\end{aligned}$$

So, $A + \bar{0} = A$, and a nearly-identical calculation shows $\bar{0} + A = A$

4. **EVERY ENDOMORPHISM HAS AN ADDITIVE INVERSE.**

Define $-A$ to be the map $x \mapsto -A(x)$. Then it is a abelian group homomorphism, as

$$\begin{aligned}
(-A)(x + y) &= -(A(x + y)) \\
&= -(A(x) + A(y)) \\
&= (-A(y)) + (-A(x)) \\
&= (-A(x)) + (-A(y)) \\
&= (-A)(x) + (-A)(y).
\end{aligned}$$

for all $x, y \in M$.

For all $x \in M$,

$$\begin{aligned}
(A + (-A))(x) &= A(x) + (-A)(x) \\
&= A(x) + (-A(x)) \\
&= 0,
\end{aligned}$$

so $A + (-A) = \bar{0}$.

5. **ADDITION COMMUTES.**

For all $x \in M$,

$$(A + B)(x) = A(x) + B(x) = B(x) + A(x) = (B + A)(x),$$

which shows that $A + B = B + A$.

Next, we show that composition is a monoid. This was already done earlier in the book, but we repeat it.

1. **MULTIPLICATION IS CLOSED.**

In other words, the composition of two abelian group homomorphisms is again an abelian group homomorphism.

For all $x, y \in M$,

$$\begin{aligned}
 (AB)(x + y) &= A(B(x + y)) \\
 &= A(B(x) + B(y)) \\
 &= A(B(x)) + A(B(y)) \\
 &= (AB)(x) + (AB)(y).
 \end{aligned}$$

So $AB \in \text{End } M$.

2. **MULTIPLICATION IS ASSOCIATIVE.**

For all $x \in M$,

$$\begin{aligned}
 (A(BC))(x) &= A((BC)(x)) \\
 &= A(B(C(x))) \\
 &= (AB)(C(x)) \\
 &= ((AB)C)(x),
 \end{aligned}$$

so $A(BC) = (AB)C$.

3. **THE IDENTITY MAP IS THE UNIT OF MULTIPLICATION.**

Let $\bar{1}$ denote the map $x \mapsto x$. Then $\bar{1}$ is an abelian group homomorphism, as

$$\bar{1}(x + y) = x + y = \bar{1}(x) + 1_{\text{End } M}(y)$$

for all $x, y \in M$.

For all $x \in M$,

$$\begin{aligned}
 (A\bar{1})(x) &= A(\bar{1}(x)) \\
 &= A(x)
 \end{aligned}$$

and

$$\begin{aligned}
 (\bar{1}A)(x) &= \bar{1}(A(x)) \\
 &= A(x),
 \end{aligned}$$

so $\bar{1}A = A\bar{1} = A$.

Finally, we check that the distributive laws hold

1. **RIGHT MULTIPLICATION DISTRIBUTES OVER ADDITION.**

For all $x \in M$,

$$\begin{aligned}
 ((A + B)C)(x) &= (A + B)(C(x)) \\
 &= A(C(x)) + B(C(x)) \\
 &= (AC)(x) + (BC)(x) \\
 &= (AC + BC)(x),
 \end{aligned}$$

so $(A + B)C = AC + BC$.

2. **LEFT MULTIPLICATION DISTRIBUTES OVER ADDITION.**

For all $x \in M$,

$$\begin{aligned}
 (A(B + C))(x) &= A((B + C)(x)) \\
 &= A(B(x) + C(x)) \\
 &= A(B(x)) + A(C(x)) \\
 &= (AB)(x) + AC(x) \\
 &= (AB + AC)(x),
 \end{aligned}$$

so $A(B + C) = AB + AC$.

This completes the theorem. □

We have some examples.

Example 1.1.3. The ring of endomorphisms of the infinite cyclic group $(\mathbb{Z}, +, 0)$ is isomorphic to $(\mathbb{Z}, +, \cdot, 1, 0)$, so $\text{End} \simeq \mathbb{Z}$.

Proof. Since \mathbb{Z} is generated by 1, it suffices to know the image of 1 to determine an endomorphism in $\text{End } \mathbb{Z}$. □

Example 1.1.4. The ring of endomorphisms of $\mathbb{Z} \times \mathbb{Z}$ is isomorphic to $M_2(\mathbb{Z})$.

Example 1.1.5. The ring of endomorphisms of $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

We have the following analogue of Cayley's theorem

Theorem 1.1.6. Any ring is isomorphic to the ring of endomorphisms of an abelian group.

Proof. Let R be a ring, and let R_+ denote its additive group. For all $a \in R$, define the left multiplication map $a_L : x \mapsto ax$. By the distributive law, $a_L(x+y) = a(x+y) = ax + ay = a_L(x) + a_L(y)$, so $a_L \in \text{End } R_+$ for all $a \in R$.

We will show that the map sending $a \mapsto a_L$ is a ring homomorphism $R \hookrightarrow \text{End } R_+$. Let $a, b \in R$. For all $x \in R_+$,

$$\begin{aligned} (a+b)_L(x) &= (a+b)x \\ &= ax + bx \\ &= a_L(x) + b_L(x) \\ &= (a_L + b_L)(x). \end{aligned}$$

and

$$\begin{aligned} (ab)_L(x) &= (ab)(x) \\ &= abx \\ &= a_L(b_L(x)) \\ &= (a_L b_L)(x), \end{aligned}$$

so $(a+b)_L = a_L + b_L$, $(ab)_L = a_L b_L$. Finally, we note that 1_L is the map $x \mapsto 1x = x$, so $1_L = 1$.

So the map $a \mapsto a_L$ is a ring homomorphism. Denote its image by R_L .

We will show that it is a monomorphism, so that $R \simeq R_L \subseteq \text{End } R_+$.

Suppose $a_L = b_L$. Then $a = a_L(1) = b_L(1) = b$, so $a = b$.

This completes the proof—by the first isomorphism theorem for rings, $R \simeq R_L$. \square

We can define the right action R_R as well.

Theorem 1.1.7. $R_L = Z(R_R)$ and $R_R = Z(R_L)$

Exercises

Exercise 1.1. Let G be a group (written multiplicatively), and let $F = G^G$ be the set of maps of G into G . If $\eta, \zeta \in F$ define $\eta\zeta$ in the usual way as the composite η following ζ . Define $1 := x \mapsto x$, $0 := x \mapsto 1$. Investigate the properties of the structure $(F, +, \cdot, 0, 1)$.

Omitted.

Exercise 1.2. Let M be an abelian group. Observe that $\text{Aut } M$ is the group of units (invertible elements) of $\text{End } M$. Use this to show that $\text{Aut } M$ for the cyclic group of order n is isomorphic to the group of cosets $\overline{m} = m + (n)$ in $\mathbb{Z}/(n)$ such that $(m, n) = 1$.

Omitted.

Exercise 1.3. Determine $\text{Aut } M$ for $M = (\mathbb{Z} \times \mathbb{Z}, +, 0)$.

Two-by-two invertible integer matrices, namely the matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that $ad - bc \in +1, -1$.

Exercise 1.4. Determine $\text{End}(\mathbb{Q}, +, 0)$.

Interesting! It should be infinite dimensional...

Exercise 1.5. In several cases we have considered, we have $\text{End}(R, +, 0) \simeq R$ for a ring R . Does this hold in general? Does it hold if R is a field?

I don't think so?

1.2 Left and right modules

Definition 1.2.1. Let R be a ring. A **left R -module** is an abelian group M together with a scaling map $\cdot : R \times M \mapsto M$ such that

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

for all $x, y \in M$ and $a, b \in R$.

Proposition 1.2.2. Any abelian group M is a \mathbb{Z} -module with the scaling map

$$ax := \begin{cases} \underbrace{x + \cdots + x}_{a \text{ times}}, & a > 0 \\ \underbrace{(-x) + \cdots + (-x)}_{-a \text{ times}}, & a < 0 \\ 0. & a = 0 \end{cases}$$

where $a \in \mathbb{Z}$ and $x \in M$.

1.3 Fundamental concepts and results

Definition 1.3.1. Fix a ring R . A **R -module homomorphism** between the two R -modules M and N is a map $\eta : M \rightarrow N$ such that η is a group homomorphism of M and N 's additive groups, and it “commutes with scaling”: $\eta(ax) = a\eta(x)$ for all $a \in R$ and $x \in M$.