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

1 Modules over a principal ideal domain

1.1 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** $\operatorname{End} M$ of an abelian group $(M, +)$ is the set of all homomorphisms $M \to M$, with ring structure given by
>
> $$(\eta\zeta)(x) \coloneqq \eta(\zeta(x)), \qquad (\eta + \zeta)(x) \coloneqq \eta(x) + \zeta(x)$$
>
> for all $\eta, \zeta \in \operatorname{End} M$ 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. 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 $A, B, C \in \operatorname{End} M$:

1. ADDITION IS CLOSED.

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

   For all $x, y \in M$,

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

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

2. ADDITION IS ASSOCIATIVE.

   For all $x \in M$,

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

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

3. THE ZERO MAP IS THE UNIT OF ADDITION.

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

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

   for all $x, y \in M$.

   For all $x \in M$,

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

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

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

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

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

   for all $x, y \in M$.

   For all $x \in M$,

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

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

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 $x, y \in M$,

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

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

2. MULTIPLICATION IS ASSOCIATIVE.

   For all $x \in M$,

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

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

3. THE IDENTITY MAP IS THE UNIT OF MULTIPLICATION.

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

$$\overline{1}(x+y) = x+y = \overline{1}(x) + 1_{\operatorname{End} M}(y)$$

   for all $x, y \in M$.

   For all $x \in M$,

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

   and

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

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

Finally, we check that the distributive laws hold

1. RIGHT MULTIPLICATION DISTRIBUTES OVER ADDITION.

   For all $x \in M$,

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

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

2. LEFT MULTIPLICATION DISTRIBUTES OVER ADDITION.

   For all $x \in M$,

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

   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 $\operatorname{End} \simeq \mathbb{Z}$.

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

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 endomorpisms 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 $a_L \in \operatorname{End} R_+$ for all $a \in R$.

We will show that the map sending $a \mapsto a_L$ is a ring homomorphism $R \hookrightarrow \operatorname{End} R_+$. 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

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

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 $R \simeq R_L \subseteq \operatorname{End} R_+$.

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, $R \simeq R_L$. □

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 $\operatorname{Aut} M$ is the group of units (invertible elements) of $\operatorname{End} M$. Use this to show that $\operatorname{Aut} M$ 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 $\operatorname{Aut} M$ 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 $\operatorname{End}(\mathbb{Q}, +, 0)$.

We have that $\operatorname{End}(\mathbb{Q}, +, 0) \simeq \mathbb{Q}$.
First, we note that

$$\begin{aligned} a \cdot \frac{p}{q} &= \overbrace{\frac{p}{q} + \cdots + \frac{p}{q}}^{a \text{ times}} \\ &= \frac{\overbrace{p + \cdots + p}^{a \text{ times}}}{q}. \\ &= \frac{ap}{q} \end{aligned}$$

for all $a \in \mathbb{Z}$ and $p/q \in \mathbb{Q}$.
Then,

$$a\frac{p}{q} = \frac{r}{s} \iff \frac{p}{q} = \frac{r}{sa},$$

as both equalities hold if and only if

$$sap = rq.$$

Finally, we have that

$$\phi\left(\frac{p}{q}\right) = \frac{p}{q}\phi(1)$$

for any homomorphism $\phi : \mathbb{Q} \to \mathbb{Q}$.

Exercise 1.5. In several cases we have considered, we have $\mathrm{End}(R, +, 0) \simeq R$ 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 $\eta : M \to N$ 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 $x \in M$.