Contents

1 Modules

We've put a lot of time and effort into understanding vector spaces over the fields $\mathbb{R}$ and $\mathbb{C}$. With our introduction to rings, we wonder if we can have some kind of analog to a vector sapce. We introduce modules and how they are generalizations of vector spaces. In the following discussion, all rings are assumed to be commutative with 1_R, all actions are left-actions, and all modules are unital.

Definition 1. Let R be a ring and M an abelian group. We say that M is a *module* over the ring R, when the following axioms hold:

For every $m, n \in M$ and $r, s \in R$,

1. $r(m+n) = rm + rn$
2. $(r+s)m = rm + sm$
3. $(r \cdot s)m = r(sm)$
4. $1_R \cdot m = m$.

There are a whole slew of examples. Perhaps the easiest one for us to understand is a vector space over a field. An $\mathbb{F}$-module, is a vector space and vice-versa.

Example 1. Let A be an abelian group. We claim that A is a $\mathbb{Z}$-module. Let $m \in \mathbb{Z}$ and $a \in A$. We define an operation on A by

$$\mathbb{Z} \times A \longrightarrow A$$
$$(m, a) \longmapsto \sum_{i=1}^{m} a \text{ for} m \geq 1.$$

One deals with $m < 0$ in the obvious way; $-1 \cdot m = -m$. Furthermore, $0_{\mathbb{Z}} \cdot a = 0$. One can show that this makes A a $\mathbb{Z}$-module. On the other hand, an arbitrary $\mathbb{Z}$-module has an underlying abelian group structure by definition.

Example 2. Any ring R is a module over itself by using the usual multiplication in R

$$R \times R \longrightarrow R$$
$$(r, s) \longmapsto r \cdot s$$

When considering R as an R-module one often writes ${}_RR$.

Example 3. Let R/I be the quotient ring of R by an ideal I. Then from above we can view R/I as a module over itself. We can also view R/I as an R-module in the following way:

$$R \times R/I \longrightarrow R/I$$
$$(r, s + I) \longmapsto (rs) + I$$

Clearly the elements in the ideal I annihlate R/I.

2 Submodules

For a subset $N \subseteq M$, we say that N is a *submodule* of M, denoted $N \leq M$, if N also has a module structure.

Lemma 1. *Let R be a ring, M an R-module, and $N \subseteq M$. Then N is a submodule of M if and only if $n_1 + rn_2 \in N$ for every $r \in R$ and $n_1, n_2 \in N$.*

Proof. "$\Rightarrow$" If N is a submodule of M, then $n_1 + rn_2 \in N$ because N is also a module.

"$\Leftarrow$" Suppose $n_1 + rn_2 \in N$ for all $r \in R$ and $n_1, n_2 \in N$. Then taking r to be the unity N is closed under sums. Letting $r = -1_R$ and $n_1 = n_2$ one sees that the elements of N have additive inverses in N. We can now see that N has an additive group structure. Taking $n_1 = 0$ we also see that N is closed under scalar multiplication. □

Lemma 2. *Let R be a ring. The submodules of ${}_RR$ are the ideals of R.*

Proof. "$\Leftarrow$" If I is an ideal of R, then $x + y \in I$ and $ry \in I$ for every $x, y \in I$ and $r \in R$ by definition. Hence $x + ry \in I$ for every $x, y \in I$ and $r \in R$, and by the previous lemma I is a submodule.

"$\Rightarrow$" Suppose N is a submodule of ${}_RR$. Then for $n_1, n_2 \in N$ and $r \in R$, $n_1 + rn_2 \in N$. Hence, N is closed under addition and $rn \in N$ for each $r \in R$ and $n \in N$. We conclude that N is an ideal. □

Since M has an underlying abelian group structure, we have no problem forming the quotient group M/N. We endow M/N with an operation from R by

$$\begin{aligned} R \times M/N &\longrightarrow M/N \\ (r, n_1 + N) &\longmapsto (r \cdot m) + N. \end{aligned}$$

One, of course, needs to assure themselves that the operation is well-defined.

3 Module Homomorphisms

As always, one wants to understand the morphisms between R-modules.

Definition 2. Let R be a ring and M, N two R-modules. We say that $\varphi : M \to N$ is an R-module homomorphism if for all $r \in R$ and $m, m' \in M$

1. $\varphi(m + m') = \varphi(m) + \varphi(m')$

2. $\varphi(rm) = r\varphi(m)$

We saw that $I \subseteq R$ was an ideal if and only if I was the kernel of a ring homomorphism. We sketch a proof of a similar results for modules.

Proposition 1. *A subset $N \subseteq M$ is a submodule if and only if it is the kernel of some R-module homomorphism.*

Proof. (Sketch.)

"$\Leftarrow$" The kernel of a ring homomorphism is a submodule because for $r \in R$ and $x, y \in \operatorname{Ker}\varphi$

- $\varphi(rx) = r\varphi(x) = 0$

- $\varphi(x + y) = \varphi(x) + \varphi(y) = 0 + 0 = 0$

"$\Rightarrow$" When N is a submodule of M, N is the kernel of the natural surjection $M \twoheadrightarrow M/N$. □

Theorem 1 (First Isomorphism Theorem)**.** *Let M and N be two R-modules and $\varphi : M \twoheadrightarrow N$ a surjective R-module homomorphism. Then*

$$M/\operatorname{Ker}\varphi \cong N$$

Proof. Define a map

$$\tau : M/\operatorname{Ker}\varphi \longrightarrow N$$
$$m + \operatorname{Ker}\varphi \longmapsto \varphi(m).$$

Claim: 1. *τ is a well-defined map.*

Suppose that m and m' are representatives of the same equivalence class. Then $m - m' \in \operatorname{Ker}\varphi$. Hence $\varphi(m - m') = \varphi(m) - \varphi(m') = 0$ so $\varphi(m) = \varphi(m')$ as desired.

Claim: 2. *τ is an R-module homomorphism*

- $\tau(rm + \operatorname{Ker}\varphi) = \varphi(rm) = r\varphi(m) = r\tau(m + \operatorname{Ker}\varphi)$

- $\tau(m + m' + \operatorname{Ker}\varphi) = \varphi(m + m') = \varphi(m) + \varphi(m') = \tau(m + \operatorname{Ker}\varphi) + \tau(m' + \operatorname{Ker}\varphi)$.

Claim: 3. *τ is a bijection*

Let $n \in N$ be arbitrary. There exists $m \in M$ such that $\varphi(m) = n$ because φ is a surjection. Hence $\tau(m + \operatorname{Ker}\varphi) = n$ and τ is also a surjection. Furthermore, $\tau(m + \operatorname{Ker}\varphi) = 0$ if and only if $\varphi(m) = 0$ which implies that $m \in \operatorname{Ker}\varphi$. □

4 Exact Sequences and Chain Complexes

We now embark on adding a powerful tool to our arsenal. That of the exact sequence. Let M_i, indexed by $i \in I$, be a collection of R-modules and $\varphi_i : M_i \to M_{i-1}$, R-module homomorphisms. The sequence

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots$$

is said to be exact if $\operatorname{Im} \varphi_{i+1} = \operatorname{Ker} \varphi_i$.

A *short exact sequence (ses)* is an exact sequence of the following form

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

- $\operatorname{Ker} f = 0$ so f is injective
- $\operatorname{Ker}(M_3 \to 0) = M_3 = \operatorname{Im} g$ so g is surjective.

We have a straight-forward example of a short exact sequence from quotient modules:

$$0 \longrightarrow N \overset{\iota}{\hookrightarrow} M \overset{\pi}{\twoheadrightarrow} M/N \longrightarrow 0$$

where ι is the inclusion map and π is the canonical projection.

One can work with sequences that are not exact, and attempt to understand how far they are from being exact, in some sense.

Definition 3. A *(chain) complex* $E^\bullet$ of R-modules is a diagram

$$\cdots \longrightarrow E^{n-1} \xrightarrow{d^{n-1}} E^n \xrightarrow{d^n} E^{n+1} \xrightarrow{d^{n+1}} \cdots$$

such that $d^{i+1} \circ d^i = 0$. That is $\operatorname{Im} d^i \subseteq \operatorname{Ker} d^{i+1}$.

Example 4. An example of a complex is

$$\cdots \longrightarrow \mathbb{Z}/8 \xrightarrow{\cdot 4} \mathbb{Z}/8 \xrightarrow{\cdot 4} \mathbb{Z}/8 \longrightarrow 0$$

One notes that $\operatorname{Ker}(\mathbb{Z}/8 \xrightarrow{\cdot 4} \mathbb{Z}/8) = \{2, 4, 6, 0\}$. Further, $\operatorname{Im}(\mathbb{Z}/8 \xrightarrow{\cdot 4} \mathbb{Z}/8) = \{4, 0\}$. Hence, the sequence is not exact. However, it does satisfy our condition that $\operatorname{Im} \subseteq \operatorname{Ker}$.

We mentioned that we can try and measure or determine how far the sequence is from being exact. This gives rise to the idea of homology.

Definition 4. We define the i^{th} homology by

$$H^i(E^\bullet) = \frac{\operatorname{Ker} d^i}{\operatorname{Im} d^{i+1}}.$$

For our example,

$$H^0 = \frac{\operatorname{Ker}(\mathbb{Z}/8 \xrightarrow{\cdot 4} \mathbb{Z}/8)}{\operatorname{Im}(\mathbb{Z}/8 \xrightarrow{\cdot 4} \mathbb{Z}/8)} \cong \mathbb{Z}/2$$

5 Shift Operators

We've introduced the following structures at this point:

- $\mathbb{F}[z]$ - the polynomials in a single variable with coefficients in a field $\mathbb{F}$. This is a PID.
- $\mathbb{F}[[z]]$ - the ring of all formal power series in a single variable.
- $\mathbb{F}(z)$ - the field of rational functions
$$\mathbb{F}(z) = \mathbb{F}[a] \oplus \mathbb{F}_-(z)$$
- $\mathbb{F}((z^{-1}))$ - the field of truncated Laurent Series. This is the field of fractions of $\mathbb{F}[[z^{-1}]]$.

$$\mathbb{F}((z^{-1})) = \mathbb{F}[z] \oplus z^{-1}\mathbb{F}[[z^{-1}]]$$

We then have the two natural projections

$$\begin{aligned} \pi_+ : \mathbb{F}((z^{-1})) &\longrightarrow \mathbb{F}[z] \\ \sum_{-\infty}^{N} \alpha_j z^j &\longmapsto \sum_{j=0}^{N} \alpha_j z^j \end{aligned}$$

and

$$\begin{aligned} \pi_- : \mathbb{F}((z^{-1})) &\longrightarrow z^{-1}\mathbb{F}[[z^{-1}]] \\ \sum_{-\infty}^{N} \alpha_j z^j &\longmapsto \sum_{-\infty}^{-1} \alpha_j z^j \end{aligned}$$

We now consider an $\mathbb{F}((z-1))$-linear map over the field $\mathbb{F}((z^{-1}))$. Well,

$$L_A : \mathbb{F}((z^{-1})) \longrightarrow \mathbb{F}((z^{-1}))$$

is completely determined by where we send the identity because $\mathbb{F}((z^{-1}))$ is a 1-dimensional $\mathbb{F}((z^{-1})$ vector space. Hence
$$(L_A f)(z) = A(z)f(z)$$
for some $A(z) \in \mathbb{F}((z^{-1}))$.

We are interested in a particular example of a Laurent operator. We define the *shift*

$$\begin{aligned} S : \mathbb{F}((z^{-1})) &\longrightarrow \mathbb{F}((z^{-1})) \\ f &\longmapsto zf \end{aligned}$$

and its inverse

$$\begin{aligned} S^{-1} : \mathbb{F}((z^{-1})) &\longrightarrow \mathbb{F}((z^{-1})) \\ f &\longmapsto z^{-1}f \end{aligned}$$

We have the direct sum decomposition
$$\mathbb{F}[z] \oplus z^{-1}\mathbb{F}[[z^{-1}]]$$

We consider $S|_{\mathbb{F}[z]}$ which we denote S^+. This works because $\mathbb{F}[z]$ is an S-invariant subspace of $\mathbb{F}((z^{-1}))$. We refer to S^+ as the *forward shift operator*. We would then like a *backward shift operator*. This operator is defined

$$\begin{aligned} S^- : z^{-1}\mathbb{F}[[z^{-1}]] &\longrightarrow z^{-1}\mathbb{F}[[z^{-1}]] \\ f &\longmapsto \pi_-(zf) \end{aligned}$$

We now outline some properties of S^+ and S^-:

1. The operator S^+ is injective because $\mathbb{F}[z]$ is a domain.
2. The operator S^+ is not surjective because the image does not contain the constant polynomials.
3. The operator S^- is not injective because every element of the form αz^{-1} is mapped to zero, $\alpha \in \mathbb{F}$.
4. The operator S^- is surjective. Let $g(z) = \sum_{j=1}^{\infty} \alpha_j z^{-j}$ is some arbitrary element of $z^{-1}\mathbb{F}[[z^{-1}]]$. Take $f(z) = \sum_{i=1}^{\infty} \beta_i z^{-i}$ where $\beta_{i+1} = \alpha_i$. Then

   $$zf(z) = \beta_1 + \sum_{i=2}^{\infty} \beta_i z^{-i+1} = \beta_1 + \sum_{i=1}^{\infty} \alpha_i z^{-i}$$

   and

   $$\pi_-(zf) = \sum_{-\infty}^{-1} \alpha_j z^j = g(z)$$

   as desired.