1 Re-interpretation of Vector Spaces

Vector spaces over a field are a special case of the more general notion of modules over a ring. Previously, we defined a vector space as a set along with two operations which obey a long list of axioms:

Definition 1a. An **(abstract) vector space** $(V, \mathbb{F}, +, \cdot)$ consists of

I. A field $\mathbb{F}$ of **scalars**
II. A set V of objects called **(abstract) vectors**
III. An rule $(+) : V \times V \to V$ for *vector addition*, satisfying
   a. *(associativity)* $u + (v + w) = (u + v) + w$
   b. *(commutativity)* $u + v = v + u$
   c. *(additive identity)* exists $0 \in V$ with $v + 0 = v$ for all $v \in V$
   d. *(additive inverse)* for all $v \in V$, exists $(-v) \in V$ with $v + (-v) = 0$
IV. A rule $(\cdot) : \mathbb{F} \times V \to V$ for *scalar multiplication*, satisfying
   a. *(scalar identity)* $1_F \cdot v = v$ for all $v \in V$
   b. *(compatibility)* $(\alpha\beta)v = \alpha(\beta(v))$
   c. *(distributes over addition)* $\alpha(v + w) = \alpha v + \alpha w$
   d. *(distributes over field addition)* $(\alpha + \beta)v = \alpha v + \beta v$

We can state these properties more concisely by noticing that Property III is equivalent to the requirement that $(V, +)$ forms a commutative group.

Definition 1b. An **(abstract) vector space** over the field $\mathbb{F}$ is a commutative group $(V, +)$ together with a rule $(\cdot) : \mathbb{F} \times V \to V$ satisfying

I. *(scalar identity)* $1_F \cdot v = v$ for all $v \in V$
II. *(compatibility)* $(\alpha\beta)v = \alpha(\beta(v))$
III. *(distributes over addition)* $\alpha(v + w) = \alpha v + \alpha w$
IV. *(distributes over field addition)* $(\alpha + \beta)v = \alpha v + \beta v$

Definitions 1a and 1b seem to present the set V as the primary object of interest, relegating the scalars $\mathbb{F}$ to the sidelines. The key to understanding modules is to turn this presumption on its head by treating $\mathbb{F}$ as the distinguished object instead.

By partial application of the scaling operator $(\cdot) : \mathbb{F} \times V \to V$, each scalar $\alpha \in \mathbb{F}$ corresponds to a linear map $\varphi_a : v \mapsto \alpha v$ from V to itself. Linear self-maps on V constitute the endomorphism ring $(\mathrm{End}(V), +, \circ)$, with pointwise addition and function composition. The vector space axioms ensure that the map $\varphi_{\boxdot} : \mathbb{F} \to (V \to V)$ from field elements to linear self-maps is a ring homomorphism. We arrive at our third and final definition,

Definition 1c. An **(abstract) vector space** over the field $\mathbb{F}$ is a commutative group $(V, +)$ together with a ring homomorphism $\varphi : \mathbb{F} \to \mathrm{End}(V)$.

The ring homomorphism defines the additive and multiplicative group actions on V by scalars from the field $\mathbb{F}$.

[0] PREREQUISITES: vector space, group, ring, endomorphism ring

2 Modules

When defining modules, we only require that the set acting on V be a ring, rather than a field.

Definition 4. A **module** over the ring R is a commutative group $(M, +)$ together with a ring homomorphism $\varphi : R \to \mathrm{End}(M)$ defining an action of R on M, where $\mathrm{End}(M)$ is the set of group homomorphisms $M \to M$.

Modules over a ring R are called ***R*-modules**, for short. An R-module is called *left* if it arises from a left action, and *right* otherwise. As for vector spaces, we could unfold this definition into a list of axioms, but this would obfuscate the real purpose of modules: Many mathematical objects happen to be rings, and modules allow us to study rings by their action on a set (much like we can study groups via their representations).

Definition 5. Let M be an R-module. An ***R*-submodule** of M is a subgroup $N \leqslant (M, +)$ closed under the ring action, $rn \in N$ for $r \in R$, $n \in N$.

Example 1. Some important examples of modules are listed below.

- If $\mathbb{F}$ is a field, then $\mathbb{F}$-modules and $\mathbb{F}$-vector spaces are identical.
- Every ring R is an R-module over itself. In particular, every field $\mathbb{F}$ is an $\mathbb{F}$-vector space. Submodules of R as a field over itself are ideals.
- If S is a subring of R with $1_S = 1_R$, every R-module is an S-module.
- If G is a commutative group of finite order m, then $m \cdot g = 0$ for all $g \in G$, and G is a $(\mathbb{Z}/m\mathbb{Z})$-module. In particular, if G has prime order p, then G is a vector space over the field $(\mathbb{Z}/p\mathbb{Z})$.
- The smooth real-valued functions $\mathcal{C}^\infty(\mathcal{M})$ on a smooth manifold form a ring. The smooth vector fields on $\mathcal{M}$ form a $\mathcal{C}^\infty(\mathcal{M})$-module.
- For a ring R, every R-algebra has natural (left/right) R-module structure given by the (left/right) ring action of R on A.

Example 2. ($\mathbb{Z}$-modules) By definition, every $\mathbb{Z}$-module is a commutative group. Likewise, every commutative group $(G, +)$ becomes a $\mathbb{Z}$-module under the ring action defined for $n \in \mathbb{Z}$, $g \in G$ by

$$n \cdot g = \begin{cases} a + a + \cdots + a & (n \text{ times}) & \text{if } n > 0 \\ 0 & & \text{if } n = 0 \\ -a - a - \cdots - a & (-n \text{ times}) & \text{if } n < 0 \end{cases}$$

We conclude that $\mathbb{Z}$*-modules and commutative groups are one in the same.*

Modules over a Polynomial Ring $\mathbb{F}[x]$

The polynomial ring $\mathbb{F}[x]$ is the space of formal linear combinations of powers of an indeterminate x, with coefficients drawn from an underlying field $\mathbb{F}$.

$$p(x) = p_0 + p_1 x + p_2 x^2 + \cdots + p_d x^m \quad (m \in \mathbb{N})$$

Polynomials form a ring[1] under entrywise addition and discrete convolution of coefficient sequences. The sum and product of $p, q \in \mathbb{F}[x]$ have coefficients

$$[p + q]_k = p_k + q_k \qquad\qquad [p \cdot q]_k = \sum_{j=0}^{\max(n,m)} p_j q_{k-j}$$

[1] the polynomial ring $\mathbb{F}[x]$ actually has the additional property of being an algebra, since $\mathbb{F}$ embeds into the center of $\mathbb{F}[x]$ via the ring homomorphism $(\alpha \in \mathbb{F}) \mapsto (\alpha \cdot 1 \in \mathbb{F}[x])$.

Consider what it would mean for an $\mathbb{F}$-vector space V to be an $\mathbb{F}[x]$-module. We need a ring homomorphism $\varphi : \mathbb{F}[x] \to \mathrm{End}(V)$ describing the action of polynomials on vectors. Since φ preserves sums and products between $\mathbb{F}[x]$ and $(\mathrm{End}(V), +, \circ)$ as rings[2], we find that the choice of a single linear map $\varphi(x) \in \mathrm{End}(V)$ determines the value of φ on arbitrary polynomials $p \in \mathbb{F}[x]$,

$$\varphi(p)v = \varphi\left(\sum_{k=1}^{m} p_k x^k\right) v = \sum_{k=1}^{m} p_k \varphi(x)^k v$$

Similarly, any choice of $\phi(x) \in \mathrm{End}(V)$ yields a valid ring homomorphism, exposing a bijection between $\mathbb{F}[x]$-modules and pairs $(V, T \in \mathrm{End}(V))$.

$$\left\{ \mathbb{F}[x]\text{-modules } V \right\} \longleftrightarrow \left\{ \begin{array}{c} \mathbb{F}\text{-vector spaces } V \text{ with a} \\ \text{linear map } T : V \to V \end{array} \right\}$$

In general, there are many different $\mathbb{F}[x]$-module structures a given $\mathbb{F}$-vector space V, each corresponding to a choice of linear $T : V \to V$.

Proposition 1. The $\mathbb{F}[x]$-submodules of an $\mathbb{F}[x]$-module V are precisely the T-invariant subspaces of V, where $T \in \mathrm{End}(V)$ denotes the action of x.

Proof. Each $\mathbb{F}[x]$-submodule of V is closed under actions by ring elements, including T. Likewise, every T-invariant subspace is closed under ring actions, which are all polynomials in T. □

3 Module Homomorphisms

Definition 6. An ***R*-module homomorphism** is a map $\phi : M \to N$ between modules which respects the R-module structure, by preserving addition and commuting with the ring action on M,

$$\begin{aligned} \phi(x+y) &= \phi(x) + \phi(y) && \forall\, x, y \in M \\ \phi(r \cdot x) &= r \cdot \phi(x) && \forall\, x \in M, r \in R \end{aligned}$$

The **kernel** of a module homomorphism is its kernel $\ker \phi = \phi^{-1}\{0_S\}$ as an additive group homomorphism. A bijective R-module homomorphism is an **isomorphism**. For any ring R, the set $\mathrm{Hom}_R(M, N)$ of homomorphisms between two R-modules forms a commutative group under pointwise addition, $(\phi + \psi)(m) \equiv \phi(m) + \psi(m)$ for $\phi, \psi \in \mathrm{Hom}_R(M, N)$. Moreover,

Proposition 2. For a commutative ring R, the group $\mathrm{Hom}_R(M, N)$ forms an R-module under the ring action $R \to \mathrm{End}(\mathrm{Hom}_R(M, N))$ given by

$$(r \cdot \phi)(m) \equiv r \cdot \phi(m) \qquad \forall\, r \in R, m \in M, \phi \in \mathrm{Hom}_R(M, N)$$

Sketch. Commutativity of R guarantees that $(r \cdot \phi) \in \mathrm{Hom}_R(M, N)$, since

$$\begin{aligned} (r \cdot \phi)(s \cdot m) &= r \cdot \phi(s \cdot m) && \text{(by definition)} \\ &= rs \cdot \phi(m) && \text{(ϕ is a homomorphism)} \\ &= sr \cdot \phi(m) && \text{(commutativity)} \\ &= s \cdot (r \cdot \phi(m)) && \text{(by definition)} \end{aligned}$$ □

[2] We take some notational shortcuts. For instance, $\phi(x)^k$ is $\phi(x)$ composed with itself k times, and p_k refers to both the element of $\mathbb{F}$ and to the map $(v \mapsto p_k v) \in \mathrm{End}(V)$.

Ring of Module Endomorphisms

Proposition 3. Endomorphisms $\mathrm{Hom}_R(M, M)$ form a unital ring, where

$$\begin{aligned} (\phi + \psi)(m) &= \phi(m) + \psi(m) && \text{(pointwise addition)} \\ (\phi\psi)(m) &= (\phi \circ \psi)(m) && \text{(composition)} \\ 1_{\mathrm{Hom}_R(M,M)} &= \mathrm{Id}_M && \text{(multiplicative identity)} \end{aligned}$$

We write $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ for the **endomorphism ring** of M.

Proposition 4. Let M be a module over a commutative ring R. The endomorphism ring $\mathrm{End}_R(M)$ forms an R-algebra, under the same ring action $r \overset{\varphi}{\mapsto} (\varphi_r : m \mapsto rm)$ which defines M as an R-module.

This property is normally stated without reference to ring homomorphisms, but in these notes we wish to emphasize that the study of modules is really the study of *ring actions*. There is at least one subtlety, though: When defining M as an R-module, we required that $\varphi_\boxdot : R \to \mathrm{End}(M, +)$ be a ring homomorphism from R to the additive group endomorphisms on $(M, +)$. Now, we are asking whether each φ_r is also an R-module homomorphism.

Proof. First, the additive group homomorphism $\varphi_r \in \mathrm{End}(M, +)$ is also a module homomorphism, since for $r, s \in R$ and $m \in M$,

$$\begin{aligned} \varphi_r(s \cdot m) &= r \cdot (s \cdot m) && \text{(by definition)} \\ &= (rs) \cdot m_1 && \text{(associativity of scalars)} \\ &= s \cdot (r \cdot m) && \text{(associativity of scalars)} \\ &= s \cdot \varphi_r(m) && \text{(by definition)} \end{aligned}$$

Futher, $\varphi_\boxdot : R \mapsto \mathrm{End}_R(M)$ sending $r \mapsto \varphi_r$ is a ring homomorphism.

$$\begin{aligned} \varphi_{r_1+r_2}(m) &= (r_1 + r_2) \cdot m && \text{(by definition)} \\ &= r_1 \cdot m + r_2 \cdot m && \text{(distributivity of scalars)} \\ &= \varphi_{r_1}(m) + \varphi_{r_2}(m) && \text{(by definition)} \\ \varphi_{r_1 r_2}(m) &= (r_1 r_2) \cdot m && \text{(by definition)} \\ &= r_2 \cdot (r_1 \cdot m) && \text{(R commutative)} \\ &= (\varphi_{r_2} \circ \varphi_{r_1})(m) && \text{(by definition)} \end{aligned}$$

Finally, each φ_r commutes with every element $\phi \in \mathrm{End}_R(M)$,

$$\begin{aligned} (\varphi_r \circ \phi)(m) &= \varphi_r(\phi(m)) && \text{(composition)} \\ &= r \cdot \phi(m) && \text{(by definition)} \\ &= \phi(r \cdot m) && \text{(module homomorphism)} \\ &= \phi(\varphi_r(m)) && \text{(by definition)} \end{aligned}$$ □

Corollary 1. By definition, every field $\mathbb{F}$ is a commutative ring. Therefore, the endomorphisms $\mathrm{End}_{\mathbb{F}}(V)$ of any $\mathbb{F}$-vector space form an $\mathbb{F}$-algebra.

4 Quotient Modules

For groups and rings, recall that quotients are well-defined only for *normal* subgroups and *multiplication-absorbing* subrings (ideals), respectively. For modules M, it turns out that *any* submodule $N \preccurlyeq M$ has a quotient M/N, and the natural projection map $\pi : M \to M/N$ is a ring homomorphism with kernel $\ker \pi = N$. Similarly, each $\mathbb{F}$-vector subspace has a quotient $\mathbb{F}$-vector space arising as the kernel of some linear map.

Proposition 5. Let R be a ring. Let $N \preccurlyeq M$ be a submodule of the R-module M. The (additive, commutative) quotient group M/N can be made into an R-module under the ring action $R \to \mathrm{End}(M/N)$ given by

$$r \cdot (x + N) = (r \cdot x) + N \qquad \forall\, r \in R, x + N \in M/N$$

The natural projection $\pi : M \to M/N$ mapping $x \mapsto x + N$ is an R-module homomorphism with kernel $\ker \pi = N$.

Theorem 1. (First Isomorphism Theorem) Let M, N be R-modules. The kernel of any module homomorphism $\phi : M \to N$ is a submodule of M, and

$$M/\ker \phi \cong \phi(M)$$

5 Free Modules

The vector space concepts of linear combinations, bases, and span all have analogues in R-module theory. We normally assume R is a ring with identity.

Definition 7. Let M be an R-module. The submodule of M **generated** by a subset $A \subset M$ is the set of finite ***R*-linear combinations**

$$RA \equiv \{r_1 a_1 + \cdots + r_m a_m \mid r_k \in R, a_k \in A, m \in \mathbb{N}\} \preccurlyeq M$$

A submodule $N = RA \preccurlyeq M$ is **finitely generated** if $A \subset M$ is finite. A **cyclic submodule** $N = Ra$ is generated by a single element $a \in M$.

Definition 8. An R-module F is **free** on the subset $A \subset F$ if each nonzero $x \in F$ expands uniquely as an R-linear combination of elements from A, in which case A is called a **basis** for F.

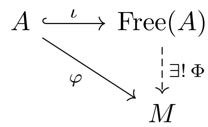
$$x = r_1 a_1 + \cdots + r_m a_m \qquad \exists!\, r_k \in R, a_k \in A, \forall\, x \in F$$

In general, more than one basis may exist. If R is commutative, every basis has the same cardinality, called the **module rank** of F. Unlike for vector spaces, not every module has a basis (not every module is free).

Universal Property of Free Modules

Recall that every linear map $T \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ between $\mathbb{F}$-vector spaces is uniquely determined by its value on $n = \dim V$ points. R-linear maps between free modules enjoy the same property, which is normally stated in the following way:

Theorem 2. (Universal Property) For any set A, there is a unique (up to isomorphism) free R-module $\mathrm{Free}(A)$ satisfying the following universal property: for any R-module M and any function $\varphi : A \to M$, there is a unique R-module homomorphism $\Phi : \mathrm{Free}(A) \to M$ such that $\Phi(a) = \varphi(a)$,



References

[1] David Steven Dummit and Richard M Foote. *Abstract Algebra*, volume 3. Wiley Hoboken, 2004.