

Artin: Linear Algebra in a Ring

James Pagan

February 2024

Contents

1	Modules	2
1.1	Definition	2
1.2	Examples of Modules	2
1.3	R-Module Homomorphisms	2
1.4	Submodules	3
2	Free Modules	5
2.1	Analogies with matrices	5
2.2	Reflections on Modules	6

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 $\mu : R \times M \rightarrow M$ (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 $f : M \rightarrow N$ between two R -modules M and N is an **R-module homomorphism** (or is **R-linear**) if for all $a \in R$ and $x, y \in M$,

$$\begin{aligned}f(x + y) &= f(x) + f(y) \\f(ax) &= af(x).\end{aligned}$$

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 $\text{Hom}_R(M, N)$ 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 $f, g \in \text{Hom}_R(M, N)$:

$$\begin{aligned}(f + g)(x) &= f(x) + g(x) \\(af)(x) &= af(x).\end{aligned}$$

We denote $\text{Hom}_R(M, N)$ by $\text{Hom}(M, N)$ if the ring R is unambiguous.

Theorem 1. $\text{Hom}_R(R, M) \cong M$

Proof. The mapping $\phi : \text{Hom}_R(R, M) \rightarrow M$ defined by $\phi(f) = f(1)$ is a homomorphism, as verified by a routine computation: for all $f, g \in \text{Hom}_R(M, N)$ and $a \in R$,

$$\begin{aligned}\phi(f + g) &= (f + g)(1) = f(1) + g(1) = \phi(f) + \phi(g) \\ \phi(af) &= (af)(1) = af(1) = a\phi(f),\end{aligned}$$

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 $u : M' \rightarrow M$ and $v : N \rightarrow N''$ induce mappings $\bar{u} : \text{Hom}(M, N) \rightarrow \text{Hom}(M', N)$ and $\bar{v} : \text{Hom}(M, N) \rightarrow \text{Hom}(M, N'')$ defined for $f \in \text{Hom}(M, N)$ as follows

$$\bar{u}(f) = f \circ u \quad \text{and} \quad \bar{v}(f) = v \circ f.$$

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:

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

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 operation $a(x + M') = ax + M'$.

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. **Compatibility:** $a(b(x + M')) = a(bx + M') = abx + M' = (ab)(x + M')$.
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 Distributivity:** $a((x + M') + (y + M')) = a((x + y) + M') = a(x + y) + M' = (ax + M') + (ay + M') = a(x + M') + a(y + M')$.

Therefore, M/M' is an R -module. Also, this operation is naturally well-defined. \square

R -module homomorphisms $f : M \rightarrow N$ induce three notable submodules:

1. **Kernel:** $\text{Ker } f = \{x \in M \mid f(x) = 0\}$, a submodule of M .
2. **Image:** $\text{Im } f = \{f(x) \mid x \in M\}$, a submodule of N .
3. **Cokernel:** $\text{Coker } f = N / \text{Im } f$, 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). $N / \text{Ker } f \cong \text{Im } f$.

Proof. Let $K = \text{Ker } f$, and define a mapping $g : M / K \rightarrow \text{Im } f$ by $g(x + K) = f(x)$. We have for arbitrary $x, y \in M$ and $a \in R$ that

$$\begin{aligned} g(x + y + K) &= f(x + y) = f(x) + f(y) = g(x + K) + g(y + K). \\ g(ax + K) &= f(ax) = af(x) = ag(x + K). \end{aligned}$$

Hence g is a homomorphism. For injectivity, suppose that $g(x + K) = g(y + K)$ — that is, $f(x) = f(y)$. Then

$$f(y - x) = f(y) - f(x) = 0,$$

so $y - x \in K$. Thus $x + K = y + K$. Surjectivity is quite clear. We conclude that g is the desired isomorphism. \square

Let $f : M \rightarrow N$ be an R -module homomorphism. Here are two special cases of the prior theorem:

1. If f is a monomorphism, then $M \cong \text{Im } f$.

2. If f is an epimorphism, then $M / \text{Ker } f \cong N$.

For a submodule $N' \subseteq \text{Im } f$, I call $M' = \{x \in M \mid f(a) \in N'\}$ the **contraction module**.

Theorem 4 (Correspondence Theorem). *Submodules of G which contain $\text{Ker } f$ correspond one-to-one with submodules of $\text{Im } f$.*

Proof. For each submodule $N' \subseteq \text{Im } f$ 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

$$f(ax) = af(x) \in N' \implies ax \in M'.$$

Hence M' is a submodule. It is clear that $\text{Ker } f \subseteq M'$, so the First Isomorphism Theorem yields that

$$N' / \text{Ker } f \cong M'.$$

Thus this construction is injective. It is surjective, since for each $\text{Ker} \subseteq N' \subseteq N$, the subgroup N' is contracted by $f(N')$. The correspondence is now established. \square

2 Free Modules

2.1 Analogies with matrices

The **free and finitely-generated R -modules** are the R -vectors with entries in R and operations defined as follows:

$$\begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} + \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix} = \begin{bmatrix} r_1 + s_1 \\ \vdots \\ r_n + s_n \end{bmatrix} \quad \text{and} \quad s \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} sr_1 \\ \vdots \\ sr_n \end{bmatrix}.$$

Analogously to fields, we can define **R -matrices** — matrices with components in R — as R -module homomorphisms from R^n to R^m . Addition and multiplication of R -matrices is defined as expected. The set of all R -module homomorphisms forms the **general linear group**:

$$GL_n(R) = \{n\text{-by-}n \text{ invertible } R\text{-matrices}\}.$$

The **determinant** of an R -module is computed in precisely the same way, and satisfies a similar property: if \mathbf{T} and \mathbf{S} are R -matrices capable of multiplication,

$$\det(\mathbf{TS}) = \det(\mathbf{T}) \det(\mathbf{S})$$

There is also the **cofactor matrix**: there exists a matrix $\text{cof}(\mathbf{T})$ such that $\mathbf{T} \text{cof}(\mathbf{T}) = \text{cof}(\mathbf{T})\mathbf{T} = \det(\mathbf{T})\mathbf{I}$.

Lemma 2. *Let \mathbf{T} be a square R -matrix. Then the following holds:*

1. \mathbf{T} is invertible if and only if $\det(\mathbf{T})$ is a unit.
2. \mathbf{T} is invertible if and only if \mathbf{T} has a one-sided inverse.
3. If \mathbf{T} is invertible, then \mathbf{T} is square.

Proof. Suppose that $\det(\mathbf{T})$ is a unit. Then $(\det(\mathbf{T})^{-1}) \operatorname{cof}(\mathbf{T})$ suffices as an inverse of \mathbf{T} by the properties of cofactor matrices; the converse holds as well. If \mathbf{T} has a one-sided inverse \mathbf{S} , then without loss of generality,

$$\det(\mathbf{T}) \det(\mathbf{S}) = \det(\mathbf{TS}) = \det(\mathbf{I}) = 1,$$

so $\det(\mathbf{T})$ is a unit; hence \mathbf{T} is invertible. Now, suppose that \mathbf{T} is invertible; if \mathbf{T} is not square, we can extend it and its inverse \mathbf{S} by adding rows (or columns) of zeroes. This yields the following equation without loss of generality:

$$\left[\begin{array}{c|c} \mathbf{T} & 0 \end{array} \right] \left[\begin{array}{c} \mathbf{S} \\ \hline 0 \end{array} \right] = \mathbf{I}.$$

This is a contradiction, since the left-hand side has determinant 0 and the right-hand side has determinant 1. \square

When R has few units, invertibility is strong condition. For instance, a \mathbb{Z} -matrix is invertible if and only if its determinant is ± 1 . Thus $GL_n(\mathbb{Z}) \subset GL_n(\mathbb{R})$; of all integer matrices that are invertible as \mathbb{R} -matrices, few are invertible as \mathbb{Z} -matrices.

2.2 Reflections on Modules

Given the similarity of free R -matrices with vector spaces, we may begin to investigate the generality of this connection. Hence, let M be an R -module. M is **finitely generated** if there exist $x_1, \dots, x_n \in M$ such that

$$M = Rx_1 + \dots + Rx_n = \{r_1x_1 + \dots + r_nx_n \mid r_1, \dots, r_n \in R\}.$$

A set of elements x_1, \dots, x_n is **independent** if

$$r_1x_1 + \dots + r_nx_n = 0 \implies r_1, \dots, r_n = 0.$$

An independent set of generators is called a **basis**. As with vector spaces, $x_1, \dots, x_n \in M$ is a basis of M if and only if all elements of M are a unique linear combination of x_1, \dots, x_n . The **canonical basis** consisting of $\mathbf{e}_1, \dots, \mathbf{e}_n$ is a basis of R^n .

If (x_1, \dots, x_n) is an ordered set of elements in M , we can define a homomorphism $R^n \rightarrow M$ defined by

$$\phi(r_1, \dots, r_n) = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = r_1 x_1 + \cdots + r_n x_n.$$

This homomorphism is injective if x_1, \dots, x_n generates M , surjective if x_1, \dots, x_n are independent, and bijective if x_1, \dots, x_n constitute a basis of R^n . Hence M has a basis of length n if and only if $M \cong R^n$.

Most modules have no basis.

A **free R-module** is a module that has a basis. A free \mathbb{Z} -module is **free Abelian group**. Finite Abelian groups are never free, since the additive order of each element is finite.