Artin: Linear Algebra in a Ring

James Pagan

February 2024

Contents

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

$$f(x + y) = f(x) + f(y)$$
$$f(ax) = af(x).$$

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

$$(f + g)(x) = f(x) + g(x)$$
$$(af)(x) = af(x).$$

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

Proposition 1. $\mathrm{Hom}_R(R, M) \cong M$

Proof. The mapping $\phi : \mathrm{Hom}_R(R, M) \to M$ defined by $\phi(f) = f(1)$ is a homomorphism, as verified by a routine computation: for all $f, g \in \mathrm{Hom}_R(M, N)$ 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 $u : M' \to M$ and $v : N \to N''$ induce mappings $\bar{u} : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N)$ and $\bar{v} : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'')$ defined for $f \in \mathrm{Hom}(M, N)$ as follows

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

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.

Proposition 2. *$\mathfrak{a}$ 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 1. *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. ☐

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

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

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

$$f(y - x) = f(y) - f(x) = 1,$$

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

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

1. If f is a monomorphism, them $M \cong \operatorname{Im} f$.

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

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

Theorem 3 (Correspondence Theorem)**.** *Submodules of G which contain* $\operatorname{Ker} f$ *correspond one-to-one with submodules of* $\operatorname{Im} f$*.*

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

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

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

$$N' \,/\, \operatorname{Ker} f \;\cong\; M'.$$

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

2 Free Modules

2.1 R-Matrices

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

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

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 $\operatorname{cof}(\mathbf{T})$ such that $\mathbf{T}\operatorname{cof}(\mathbf{T}) = \operatorname{cof}(\mathbf{T})\mathbf{T} = \det(\mathbf{T})\mathbf{I}$.

Lemma 1. *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. □

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 Free 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 $x_1, \ldots, x_n \in M$ such that

$$M \;=\; Rx_1 + \cdots + Rx_n \;=\; \{r_1x_1 + \cdots + r_n \mid r_1, \ldots, r_n \in R\}.$$

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

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

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

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

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

This homomorphism is injective if $x_1, \ldots, x_n$ generates M, surjective if $x_1, \ldots, x_n$ are independent, and bijective if $x_1, \ldots, x_n$ 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.

We arrive at the definition of this section: **free R-module** is a module that has a basis. Compare this definition to Atiyah's delineated in AbstractAlgebra/atiyah2.tex. A free $\mathbb{Z}$-module is **free Abelian group**. Finite Abelian groups are never free — if desired without Atiyah's logic, this is obtained by observing that each element has finite order:

$$o(x_1)x_1 + \cdots o(x_n)x_n \;=\; 0 + \cdots + 0 \;=\; 0$$

The **rank** of a free R-module M is the cardinality of a basis of M. The rank of a free R-module is analogous to the dimension of a vector space.

2.3 Matrices in Free Modules

Let $\mathbf{B}$ be the basis of a free M-module M. The **coordinate vector** X of an element $\mathbf{v} \in M$ is the unique column vector such that $\mathbf{v} = \mathbf{B}X$. If $\mathbf{B}'$ is a change of basis, the relevant formula is $\mathbf{B}' = \mathbf{B}P$. We assert the following proposition without proof:

Proposition 3. *The following two properties of bases hold:*

1. *A matrix* $\mathbf{T}$ *of a change-of-basis in a free module is an invertible R-matrix.*
2. *All bases of a free R-module have the same cardinality.*

Let M and N be free R-modules with bases $\mathbf{B} = (x_1, \ldots, x_n)$ and $\mathbf{C} = (y_1, \ldots, y_m)$ respectively. Then all R-module homomorphisms $f : M \to N$ admit the form of left-multiplication by an m-by-n R-matrix $\mathbf{T} = (t_{ij})$, with components given by

$$f(y_j) \;=\; \sum_{i=1}^{n} x_i t_{ij}$$

If X is the coordinate vector of $\mathbf{v} \in M$ — namely, if $\mathbf{v} = \mathbf{B}X$ — then $Y = \mathbf{T}X$ is the coordinate vector of its image.

$$\begin{tikzcd} R^n \arrow[r, "\mathbf{T}"] \arrow[d, "\mathbf{B}"] & R^m \arrow[d, "\mathbf{C}"] \\ M \arrow[r, "f"] & N \end{tikzcd} \quad \Longleftrightarrow \quad \begin{tikzcd} X \arrow[r, dashed] \arrow[d, dashed] & Y \arrow[d, dashed] \\ \mathbf{v} \arrow[r, dashed] & f(\mathbf{v}) \end{tikzcd}$$

Let the bases $\mathbf{B}$ and $\mathbf{C}$ change by invertible R-matrices $\mathbf{S}$ and $\mathbf{R}$. Then if $\mathbf{T}$ is the R-matrix of $f : M \to N$, the new formula for $\mathbf{T}$ is the same for vector spaces: $\mathbf{T}' = \mathbf{R}^{-1}\mathbf{T}\mathbf{S}$.

3 Diagonalizing Integer Matrices

The critical question is as follows: given an m-by-n $\mathbb{Z}$-matrix $\mathbf{T}$ and $\mathbf{B} \in \mathbb{Z}^m$, when does there exist $\mathbf{A} \in \mathbb{Z}^n$ such that

$$\mathbf{A}\mathbf{T} = \mathbf{B}?$$

The most important of these questions is when $\mathbf{A}\mathbf{T} = \mathbf{0}$. In a field, one often performs row reduction — but deprived of multiplicative inverses, most row reductions are not allowed. Rather, we allow both row *and* column reduction. One is permitted to perform any of the following operations:

1. Add an integer multiple of a row to a row or a column to a column.
2. Interchange two rows or two columns.
3. Multiply a row or column by -1.

Any such operation can be performed by multiplying $\mathbf{T}$ by an **elementary integer matrix**, which is always invertible. Therefore the final result of a sequence of operations has the form

$$\mathbf{T}' = \mathbf{Q}^{-1}\mathbf{T}\mathbf{P},$$

where $\mathbf{Q}^{-1}$ and $\mathbf{T}$ are invertible $\mathbb{Z}$-matrices of the appropriate sizes. $\mathbf{Q}^{-1}$ documents row operations, while $\mathbf{P}$ dictates column operations: those in $\mathbf{P}$ are multiplied in the same order as performed, while those in $\mathbf{Q}$ are in *reverse* order.

Theorem 4.

Proof. $\square$