

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	R-Matrices	5
2.2	Free Modules	6
2.3	Matrices in Free Modules	7
3	Diagonalizing Integer Matrices	8
3.1	Subgroups of Free Abelian Groups	10
4	Presentation Matrices	11
4.1	Translating between Presentations and Modules	12

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.

Proposition 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 .

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:

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

The rest of the multiplicative module conditions follow from the ring axioms. \square

The following proof outlines the construction of **quotient modules**:

Proposition 3. 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 1 (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 2 (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 R-Matrices

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

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

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 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. \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 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 $x_1, \dots, x_n \in M$ 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 $\mathbf{B} = (x_1, \dots, x_n)$ is an ordered set of elements in M , we can define a homomorphism $R^n \xrightarrow{\mathbf{B}} M$ defined by

$$\mathbf{B}X = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = a_1x_1 + \cdots + a_nx_n.$$

This homomorphism is injective if elements of \mathbf{B} is independent, surjective \mathbf{B} generates M , and bijective if \mathbf{B} 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 4. *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 $\mathbf{B} = (x_1, \dots, x_n)$ and $\mathbf{C} = (y_1, \dots, y_m)$ respectively. Then all R -module homomorphisms $f : M \rightarrow N$ 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.

$$\begin{array}{ccc} R^n & \xrightarrow{\mathbf{T}} & R^m \\ \downarrow \mathbf{B} & & \downarrow \mathbf{C} \\ M & \xrightarrow{f} & N \end{array} \iff \begin{array}{ccc} X & \dashrightarrow & Y \\ \downarrow & & \downarrow \\ \mathbf{v} & \dashrightarrow & f(\mathbf{v}) \end{array}$$

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 $f : M \rightarrow N$, 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 a vector $\mathbf{B} \in \mathbb{Z}^m$, when does there exist $\mathbf{A} \in \mathbb{Z}^n$ such that

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

The most important of these questions is when $\mathbf{T}\mathbf{A} = \mathbf{0}$. 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, that being any of the following:

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. 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 3. *Let \mathbf{T} be an m -by- n integer matrix. Then there exist invertible matrices P and Q such that $Q^{-1}\mathbf{T}P$ is diagonal — say,*

$$\left[\begin{array}{c} \left[\begin{array}{ccc} d_1 & & \\ & \ddots & \\ & & d_k \end{array} \right] \\ \left[\begin{array}{c} \\ \\ 0 \end{array} \right] \end{array} \right],$$

where d_i are positive and $d_1 \mid \cdots \mid d_k$.

Proof. We present a rather unusual proof: an algorithmic one. The strategy is to reduce \mathbf{A} to a matrix of the form

$$\begin{bmatrix} d_1 & \cdots & 0 \\ \vdots & \begin{bmatrix} \mathbf{M} \end{bmatrix} \\ 0 \end{bmatrix}, \quad (1)$$

where \mathbf{M} extends down to the bottom of the matrix (hard to draw!).

1. **Step 1:** Permute the rows and columns such that the a_{ij} with the smallest absolute value to the upper left corner. If necessary, multiply by -1 such that this element is positive.
2. **Step 2:** If the first column contains a nonzero element a_{i1} , divide it by a_{11} : we have

$$a_{i1} = a_{11}q + r,$$

where $a_{11} > r \geq 0$. If $r > 0$, perform the relevant row operation such that a_{i1} becomes r and go to Step 1. If $r = 0$, then repeat Step 2. If there are no nonzero elements, proceed to Step 3.

3. **Step 3:** If the first row contains a nonzero element a_{1j} , divide it by a_{11} : we have

$$a_{1j} = a_{11}q + r,$$

where $a_{11} > r \geq 0$. If $r > 0$, perform the relevant column operation such that a_{1j} becomes r and go to Step 1. If $r = 0$, then repeat Step 3. If there are no nonzero elements, proceed to Step 4.

4. **Step 4:** We attain a matrix of the form in Equation (1). Suppose that some element of \mathbf{M} is not divisible by d_1 . Add this column into the first column and return to Step 1; this will yield an a_{11} of smaller absolute value. If no such elements exist, proceed to Step 5.
5. **Step 5:** An easy induction on argument on $\max\{m, n\}$ now implies that \mathbf{T} can be factored into the required form.

Observe that we exclusively return to earlier steps when $|a_{11}|$ decreases. This can happen only finitely many times, so no step will ever repeat infinitely often. Then this algorithm indeed yields us a matrix of the desired form. \square

This proof isn't exactly rigorous, but it's still quite cool. I think you could formalize this via the classification of finitely-generated modules over PIDs. In any case, it ensures the existence of invertible integer matrices \mathbf{Q} and \mathbf{P} such that for all $\mathbf{T} \in \mathcal{L}(\mathbb{Z}^n, \mathbb{Z}^n)$, we have

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

where \mathbf{T}' has the form of Theorem 3.

We are ready to solve the equation $\mathbf{T}\mathbf{A} = \mathbf{B}$.

Proposition 5. *Let $\mathbf{T}' = \mathbf{Q}^{-1}\mathbf{T}\mathbf{P}$ as before. Then the following hold:*

1. *The integer solutions to the equation $\mathbf{T}'\mathbf{A}' = \mathbf{0}$ are the vectors \mathbf{A} whose first k components are 0.*
2. *The integer solutions to the equation $\mathbf{T}\mathbf{A} = \mathbf{0}$ are those of the form $\mathbf{A} = \mathbf{P}\mathbf{A}'$, where $\mathbf{T}'\mathbf{A}' = \mathbf{0}$.*
3. *The image W' of multiplication by \mathbf{T}' is the integer combinations of the vectors $d_1\mathbf{e}_1, \dots, d_k\mathbf{e}_k$.*
4. *The image W of multiplication by \mathbf{T} is the integer combinations of the vectors $\mathbf{Q}(d_1\mathbf{e}_1), \dots, \mathbf{Q}(d_k\mathbf{e}_k)$.*

Proof. (1) follows from the fact that \mathbf{T}' is diagonal: the equation $\mathbf{T}'\mathbf{A}'$ for $\mathbf{A} = (a_1, \dots, a_n)$ reads

$$d_1a_1 = 0, \quad d_2a_2 = 0, \quad \dots \quad d_ka_k = 0.$$

Hence there exists a solution if and only if $a_1 = \dots = a_k = 0$. Both (2) and (4) can be viewed as change of bases — in which case, the matrix \mathbf{P} carries the kernel of \mathbf{T} to the kernel of \mathbf{T}' , while \mathbf{Q} carries the image of \mathbf{T}' to the image of \mathbf{T} .

As for (3), it is quite easy to deduce that \mathbf{T}' maps all $\mathbf{A} = (a_1, \dots, a_n)$ to the vector $(d_1a_1, \dots, d_ka_k, 0, \dots, 0)$. The vectors $d_1\mathbf{e}_1, \dots, d_k\mathbf{e}_k$ clearly span this space. \square

Isn't this solution so simple and elegant? This section discussed computation and theory together, like some cosmic marble cake. But I digress: the basis of vectors described in (4) is not unique. I'm not sure if the matrix \mathbf{A}' is unique, but it seems like it should be?

3.1 Subgroups of Free Abelian Groups

Theorem 4 on diagonalization of \mathbb{Z} -matrices describes homomorphisms of Abelian groups.

Corollary 1. *Let $\phi : G \rightarrow H$ be a homomorphism of free Abelian groups. Then there exist bases of G and H such that the matrix of ϕ is diagonal.*

This section would ideally discuss R -submodules of free R -modules, where R is a principal ideal domain. Unfortunately, integer matrices are no help here; the proof of Theorem 4 relied upon the Euclidean algorithm. Thus we instead focus on \mathbb{Z} -modules.

Theorem 4. *Let G be a free Abelian group of rank n and let $H \subseteq G$ be a subgroup. Then H is a free Abelian group of rank n or smaller.*

Proof. By Theorem **INSERT NUMBER HERE!**, H is finitely generated. Thus let $\mathbf{G} = (g_1, \dots, g_m)$ and $\mathbf{H} = (h_1, \dots, h_n)$ be bases of G and H . Thus if we set $h_j = \sum_i g_i a_{ij}$, the elements a_{ij} form the components of the \mathbf{T} matrix associated with the inclusion mapping $i : G \rightarrow H$:

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{\mathbf{T}} & \mathbb{Z}^n \\ \downarrow \mathbf{H} & & \downarrow \mathbf{G} \\ H & \xrightarrow{i} & G \end{array}$$

Since \mathbf{G} is a basis, the right-hand arrow is bijective; since \mathbf{H} generates H , the left-hand arrow is surjective.

Diagonalize \mathbf{T} to the form $\mathbf{T}' = \mathbf{Q}^{-1}\mathbf{T}\mathbf{P}$ for invertible matrices \mathbf{P} and \mathbf{Q} . Thus we can interpret \mathbf{Q} as a change of basis in \mathbb{Z}^m ; since our original choice of \mathbf{G} and \mathbf{H} were arbitrary, we can substitute them into our commutative diagram. We find an isomorphism $\mathbb{Z}^m \cong H$, so H is free. \square

This proof actually misses a few edge cases — but frankly I just don't give a shit right now. I'll return to this over the weekend.

4 Presentation Matrices

Left multiplication by an m -by- n R -matrix \mathbf{T} induces an R -module homomorphism

$$R^n \xrightarrow{\mathbf{T}} R^m.$$

The image of \mathbf{T} consists of all linear combinations of the columns of \mathbf{T} with coefficients in the ring; we may denote this ring by $\mathbf{T}R^n$. We say that the quotient module $M = R^m / \mathbf{T}R^n$ is **presented** by \mathbf{T} .

More generally, any isomorphism $\sigma : R^m / \mathbf{T}R^n \rightarrow M$ is a **presentation** of M , where the R -matrix \mathbf{T} is a **presentation matrix** of M . For instance, C_5 is presented by the integer matrix $[5]$ since $C_5 \cong \mathbb{Z} / 5\mathbb{Z}$.

We can utilize the canonical epimorphism $\pi : R^m \rightarrow R^m / \mathbf{T}R^n$ to interpret M as follows:

Proposition 6. Let $\pi : R^m \rightarrow R^m / \mathbf{T}R_n$ be the canonical epimorphism. Then

1. M is generated by $\mathbf{B} = (\mathbf{e}_1, \dots, \mathbf{e}_m)$, the images of the standard basis of R^m .
2. If $\mathbf{Y} = (y_1, \dots, y_m) \in R^m$, the element $\mathbf{B}\mathbf{Y} = y_1\mathbf{e}_1 + \dots + y_m\mathbf{e}_m$ is zero if and only if \mathbf{Y} is a linear combination of the columns of \mathbf{T} — which is to say, if and only if \mathbf{Y} lies in the image of \mathbf{T} .

Proof. (1) is a trivial consequence of the surjectivity of π . As per (2), we have that

$$\begin{aligned} \mathbf{B}\mathbf{Y} = \mathbf{0} &\iff \mathbf{B}\mathbf{Y} \in \mathbf{T}R_n \\ &\iff \mathbf{Y} \text{ lies in the image of } \mathbf{T} \\ &\iff \mathbf{Y} \text{ is a linear combination of the columns of } \mathbf{T}. \end{aligned}$$

This completes the proof. □

If a module M is generated by a set $\mathbf{B} = (x_1, \dots, x_m)$, we call an element $\mathbf{Y} = (y_1, \dots, y_m) \in R^m$ such that $\mathbf{B}\mathbf{Y} = y_1x_1 + \dots + y_mx_m = 0$ a **relation vector** of the generators. The equation $y_1x_1 + \dots + y_mx_m = 0$ is called a **relation**. A set S of relations is **complete** if each relation is a linear combination of relations in S .

Example 1. Consider an Abelian group G generated by a, b, c with the complete set of relations

$$\begin{aligned} 3a + 2b + c &= 0 \\ 8a + 4b + 2c &= 0 \\ 7a + 6b + 2c &= 0 \\ 9a + 6b + c &= 0. \end{aligned}$$

This group is presented by the following matrix:

$$\mathbf{T} = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix}$$

Its columns are the coefficients of the relations described above: $(x_1, x_2, x_3)\mathbf{T} = (0, 0, 0)$.

4.1 Translating between Presentations and Modules

We now delineate a method to find a presentation for an R -module M . We make two assumptions, both of which are easily satisfied if R is Noetherian:

1. M is finitely generated — say, by $\mathbf{B} = (x_1, \dots, x_m)$.
2. The module W of relations of \mathbf{B} is finitely generated.

The generators \mathbf{B} entail an epimorphism $R^m \xrightarrow{\mathbf{B}} M$ that maps a column vector $\mathbf{Y} = (y_1, \dots, y_m)$ to the element $y_1x_1 + \dots + y_mx_m$. The kernel of this homomorphism is W : the module of relations of \mathbf{B} . By the First Isomorphism Theorem, we have

$$M \cong R^m / W.$$

We turn our attention to W . Since W is finitely generated, there exists a set of generators $\mathbf{C} = (w_1, \dots, w_n)$ from which we obtain an epimorphism $R^n \xrightarrow{\mathbf{C}} W$. The generators $\mathbf{w}_i \in R^m$ may be arranged into a matrix as follows:

$$\mathbf{T} = \begin{bmatrix} \vdots & \vdots & \cdots & \vdots \\ \mathbf{w}_1 & \mathbf{w}_2 & \cdots & \mathbf{w}_n \\ \vdots & \vdots & \cdots & \vdots \end{bmatrix}.$$

This n -by- m R -matrix \mathbf{T} is a composition of $R^n \rightarrow W$ with the embedding $W \subset R^m$. By construction, its image is W — which we may denote as $\mathbf{T}R^n$. Thus we have

$$M \cong R^m / W = R^m / \mathbf{T}R^n.$$

\mathbf{T} is a presentation of M . Observe that since \mathbf{T} depends on \mathbf{B} and \mathbf{C} , there are many potential presentations of M . In fact:

Proposition 7. *Let \mathbf{T} be an m -by- n presentation matrix of an R -module M . Then the following matrices \mathbf{T}' also present M :*

1. $\mathbf{T}' = \mathbf{Q}^{-1}\mathbf{T}$, where $\mathbf{Q} \in GL_m(R)$.
2. $\mathbf{T}' = \mathbf{TP}$, where $\mathbf{P} \in GL_n(R)$.
3. \mathbf{T}' obtained by deleting a column of zeroes.
4. If the j -th column of \mathbf{T} is \mathbf{e}_i , the matrix \mathbf{T}' obtained by deleting row i and column j .

Proof. The proofs originate from the following observations:

1. The change of \mathbf{T} to $\mathbf{Q}^{-1}\mathbf{T}$ corresponds to a change of basis in R^m — in other words, an isomorphism.
2. The change of \mathbf{T} to \mathbf{TP} corresponds to a change of basis in R^n — in other words, an isomorphism.

3. A column of zeroes corresponds to the trivial relation, which can be omitted.
4. A column of \mathbf{T} equal to \mathbf{e}_i corresponds to the relation $\mathbf{B}(\mathbf{e}_i) = 0$. The zero element is useless as a generator — so we can simply cleave it away from the generating set and the relations. Doing so changes R^n and R^m to R^{n-1} and R^{m-1} , and changes the matrix \mathbf{T} by deleting the i -th row and j -th column.

This concludes the proof. □

This provides a clean method for determining an R -module from its presentation. For the Abelian group in our example, it reduces to

$$\begin{aligned} \mathbf{T} = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix} &\implies \begin{bmatrix} 1 & 2 & 2 & 1 \\ 0 & 0 & 2 & 4 \\ 0 & 2 & 1 & 6 \end{bmatrix} \implies \begin{bmatrix} 0 & 2 & 4 \\ 2 & 1 & 6 \end{bmatrix} \implies \begin{bmatrix} -4 & 0 & -8 \\ 2 & 1 & 6 \end{bmatrix} \\ &\implies \begin{bmatrix} -4 & -8 \end{bmatrix} \implies \begin{bmatrix} 4 & 0 \end{bmatrix} \implies \begin{bmatrix} 4 \end{bmatrix}. \end{aligned}$$

Thus \mathbf{T} presents the Abelian group \mathbb{Z}_4 .