

# Linear algebra on integral domains

Pedro Resende

## Abstract

Support notes for the MMAC course “Modules and Representations” of IST in the academic year 2024/2025.

## Contents

0	Introduction	2
1	Free modules and bases	2
2	Universal property	4
3	“Linear algebra” over commutative rings	7
4	“Linear algebra” over integral domains	9
5	Solutions to some exercises	11

## 0 Introduction

Modules over arbitrary rings are similar to vector spaces in many respects, but certainly not so in others. An immediate difference is that, for a field  $F$ , every finitely generated  $F$ -module is a finite dimensional vector space, and thus it is a free  $F$ -module. However, not every finitely generated  $R$ -module is free in general. For instance  $\mathbb{Z}/n\mathbb{Z}$  is a finitely generated  $\mathbb{Z}$ -module (in fact a cyclic module generated by  $\bar{1}$ ), but it is certainly not free.

The purpose of these notes is to introduce free modules in general, and in particular for integral domains, and to recast the role of well known concepts of linear algebra, namely matrices and determinants, in this more general context.

From now on  $R$  is a fixed but arbitrary unital ring.

## 1 Free modules and bases

In analogy with the notion of *linear expansion* of a subset of a vector space, for arbitrary modules we have:

§1. DEFINITION. Let  $M$  be an  $R$ -module and  $A \subset M$  a set. The *submodule generated by  $A$* , denoted by  $RA$ , is defined to be the set of all the finite linear combinations of elements of  $A$ :

$$RA = \{0\} \cup \bigcup_{n \in \mathbb{Z}_{\geq 1}} \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R, a_i \in A\}.$$

§2. EXERCISE. Verify, using the submodule criterium, that  $RA$  is indeed a submodule of  $M$ . Verify also that it is the least submodule that contains  $A$ . Would the latter be true if  $R$  were not unital?

§3. DEFINITION. Let  $M$  be an  $R$ -module. A subset  $A \subset M$  is a set of *generators* for  $M$  if  $RA = M$ . Then  $M$  is *finitely generated* if it admits a finite set of generators, and *cyclic* if it can be generated by a single element  $a \in M$ ; that is,

$$M = Ra = \{ra \mid r \in R\}.$$

§4. DEFINITION. Let  $M$  be an  $R$ -module, and let  $A \subset M$ . Then  $M$  is said to be *freely generated* by  $A$ , or *free* on  $A$ , if for all  $m \neq 0$  there is a unique

finite subset  $\{a_1, \dots, a_n\} \subset A$  ( $n \geq 1$ ) and, for each  $i$ , a unique  $r_i \in R \setminus \{0\}$ , such that

$$m = \sum_{i=1}^n r_i a_i.$$

If this happens then  $A$  is said to be a *basis* of  $M$ .

A more elegant way of rephrasing this definition is the following, where by *support* of a function  $f : A \rightarrow R$  is meant the set  $\text{supp } f \subset A$  defined by

$$\text{supp } f = f^{-1}(R \setminus \{0\}),$$

and  $f$  is said to be *finitely supported* if  $\text{supp } f$  is a finite set (possibly even empty).

§5. DEFINITION. Let  $M$  be an  $R$ -module, and let  $A \subset M$ . Then  $M$  is said to be *freely generated* by  $A$ , or *free* on  $A$ , if for all  $m$  there is a unique finitely supported function  $f : A \rightarrow R$  such that

$$m = \sum_{a \in A} f(a)a.$$

(For  $m = 0$  the function  $f$  is zero everywhere.)

§6. REMARK. The finitely supported function in the previous definition gives us the “coordinate” of  $m$  relative to each “basis vector”  $a$ .

§7. DEFINITION. Let  $A$  be a set. The set of all the finitely supported functions  $f : A \rightarrow R$  is denoted by  $F_R(A)$ .

Notice that the assignment  $f \mapsto \sum_{a \in A} f(a)a$  in Definition 5 always defines a function  $\varphi : F_R(A) \rightarrow M$ , regardless of whether  $A$  is a basis of  $M$  or not. Let us call this the *canonical function* from  $F_R(A)$  to  $M$  (relative to the subset  $A \subset M$ ). We have the following obvious fact:

§8. PROPOSITION. Let  $M$  be an  $R$ -module,  $A \subset M$  any subset, and  $\varphi : F_R(A) \rightarrow M$  the canonical function. Then  $A$  generates  $M$  (i.e.,  $RA = M$ ) if and only if  $\varphi$  is surjective. And  $A$  freely generates  $M$  if and only if  $\varphi$  is a bijection.

But more can be said:

§9. PROPOSITION.  $F_R(A)$  is an  $R$ -module, and the canonical function  $\varphi : F_R(A) \rightarrow M$  is a homomorphism of  $R$ -modules. Moreover, it is the only homomorphism of  $R$ -modules from  $F_R(A)$  to  $M$  such that  $\varphi(\delta_a) = a$  for all  $a \in A$ .

*Proof.* (Exercise.) Begin by showing that  $F_A(A)$  is a submodule of the function module  $R^A$ . ■

§10. COROLLARY.  $M$  is generated by  $A$  if and only if  $\varphi$  is a surjective homomorphism, and it is freely generated by  $A$  if and only if  $\varphi$  is an isomorphism. Hence, if  $M$  is free on  $A$  then it is isomorphic to  $F_R(A)$ .

From now on let us denote by  $\tilde{A} \subset F(A)$  the set of all  $\delta_a$  with  $a \in A$ .

§11. THEOREM.  $M$  is a free module if and only if there is a set  $A$  such that  $M \cong F_A(A)$ . In particular,  $F_A(A)$  is a free module with basis  $\tilde{A}$ .

*Proof.* Let  $A \subset M$  be a basis. Then, by the previous corollary,  $M \cong F_R(A)$ . Conversely, assume that there is a set  $A$  (not necessarily contained in  $M$ ) such that  $M \cong F_R(A)$ . Let  $\xi : F_R(A) \rightarrow M$  be an isomorphism, and let  $A' = \xi(\tilde{A}) \subset M$ . Then  $A'$  is a basis of  $M$ , and therefore  $M$  is free. ■

## 2 Universal property

So far we have tried to see when it is that a subset  $A$  of a given module  $M$  is a basis of that module. But we can ask another question: given an arbitrary set  $A$ , which is not a priori contained in any module, can we always find a module containing  $A$  as a basis? Here we shall tackle this question, and see that the answer is yes, provided we accept a solution where only an isomorphic copy of the set  $A$  is contained in the module to be constructed.

In fact what we have seen so far gives us the answer to the question we have just asked. Given a set  $A$ , the module  $F_R(A)$  is free and it “contains”  $A$  or, more precisely, it contains the basis  $\tilde{A}$ , which is in bijection with  $A$ .

The following gives us the *universal property* of  $F_A(A)$ :

§12. THEOREM. Let  $A$  be a set and  $\eta : A \rightarrow F_A(A)$  the function such that  $\eta(a) = \delta_a$  for all  $a \in A$ . Then for any other module  $M$ , and any function  $\theta : A \rightarrow M$ , there is a unique homomorphism of modules  $\theta^\# : F_R(A) \rightarrow M$

such that  $\theta^\#(\delta_a) = \theta(a)$  for all  $a \in A$ :

$$\begin{array}{ccc} A & \xrightarrow{\eta} & F(A) \\ & \searrow \theta & \downarrow \theta^\# \\ & & M \end{array}$$

*Proof.* Exercise. ■

This shows that the pair  $(F_R(A), \eta)$  is an example of a universal arrow, namely from the set  $A$  to the forgetful functor  $U : R\text{-Mod} \rightarrow \text{Set}$ , in the sense of the following general definition:

§13. DEFINITION. Let  $C$  and  $D$  be categories, let  $U : D \rightarrow C$  be a functor, and let  $x \in C_0$ . By a *universal arrow* from  $x$  to  $U$  is meant a pair  $(\bar{x}, \eta)$  where  $\bar{x} \in D_0$  and  $\eta : x \rightarrow U\bar{x}$ , such that for all other pairs  $(y, \theta)$  where  $y \in D_0$  and  $\theta : x \rightarrow Uy$  there is a unique arrow  $\theta^\# : \bar{x} \rightarrow y$  in  $D$  such that  $U\theta^\# \circ \eta = \theta$ :

$$\begin{array}{ccc} x & \xrightarrow{\eta} & U\bar{x} \\ & \searrow \theta & \downarrow U\theta^\# \\ & & Uy \end{array} \quad \begin{array}{c} \bar{x} \\ \downarrow \theta^\# \\ y \end{array}$$

§14. REMARK. Consider the *comma category*  $(x \downarrow U)$  whose objects are the pairs  $(y, \eta_y)$  such that  $y \in D_0$  and  $\eta_y : x \rightarrow Uy$  is a morphism in  $C$ , and whose morphisms  $f : (y, \eta_y) \rightarrow (z, \eta_z)$  are the morphisms  $f : y \rightarrow z$  such that  $Uf \circ \eta_y = \eta_z$ :

$$\begin{array}{ccc} & & Uy \\ & \nearrow \eta_y & \downarrow Uf \\ x & & Uz \\ & \searrow \eta_z & \end{array}$$

Then a universal arrow from  $x$  to  $U$  is the same as an initial object in  $(x \downarrow U)$  (exercise: check this). It follows that universal arrows are unique up to an isomorphism; in particular, if  $(\bar{x}_1, \eta_1)$  and  $(\bar{x}_2, \eta_2)$  are universal arrows from the same object  $x$  to the functor  $U$  we have  $\bar{x}_1 \cong \bar{x}_2$  in  $D$ .

§15. EXERCISE. Verify that  $(x \downarrow U)$  is a category — think of it as a category of objects of  $D$  with structure; each object  $y \in D_0$  is equipped with

the structure  $\eta_y : x \rightarrow Uy$ , and the morphisms of  $(x \downarrow U)$  are the morphisms of  $D$  that respect that structure.

§16. EXERCISE. Let  $C$  and  $D$  be categories, and  $U : D \rightarrow C$  a functor. Assuming that for every  $x \in C_0$  there is a universal arrow from  $x$  to  $U$ , prove that there is a functor  $F : C \rightarrow D$ . Hint: for each  $x \in C_0$  choose a universal arrow  $(\bar{x}, \eta_x)$  from  $x$  to  $U$  and define  $F(x)$  to be  $\bar{x}$ ; and for each  $f : x \rightarrow y$  in  $C_1$  define  $F(f)$  to be  $(\eta_y \circ f)^\sharp$ :

$$\begin{array}{ccc}
 C & \xleftarrow{U} & D \\
 \\
 \begin{array}{ccc}
 x & \xrightarrow{\eta_x} & U\bar{x} \\
 \downarrow f & \searrow \eta_y f & \downarrow U(\eta_y f)^\sharp \\
 y & \xrightarrow{\eta_y} & U\bar{y}
 \end{array} & & \begin{array}{c}
 \bar{x} \\
 \vdots (\eta_y f)^\sharp \\
 \bar{y}
 \end{array}
 \end{array}$$

§17. EXAMPLE. For a function  $\phi : A \rightarrow B$  the corresponding homomorphism of modules  $F(\phi) : F(A) \rightarrow F(B)$  is given by

$$F(\phi)(f) = \sum_{a \in A} f(a)\phi(a).$$

§18. DEFINITION. Let  $C$  and  $D$  be categories. An *adjunction* from  $C$  to  $D$  consists of a functor  $U : D \rightarrow C$  and, for each  $x \in C_0$ , a universal arrow  $(\bar{x}, \eta_x)$  from  $x$  to  $U$ . Then  $U$  is called the *right adjoint* functor of the adjunction, and the functor  $F : C \rightarrow D$  of §16 is the *left adjoint* functor of the adjunction.

§19. EXERCISE. Describe an adjunction from  $Set$  to  $Set_*$ . ( $Set_*$  is the category of *pointed sets* — each object is a set  $X$  with a designated point  $x \in X$ , and an arrow  $f : (X, x) \rightarrow (Y, y)$  is a function  $f : X \rightarrow Y$  such that  $f(x) = y$ .)

§20. EXERCISE. Describe an adjunction from  $Set$  to the category of monoids  $Mon$ . Hint: for each set  $X$  consider the monoid  $X^*$  of all the strings written with “letters” from  $X$  — the empty string  $\varepsilon$  is the multiplicative identity 1.

§21. EXERCISE. Describe an adjunction from  $Grp$  to  $Ab$  whose right adjoint is the inclusion functor  $I : Ab \rightarrow Grp$ .

### 3 “Linear algebra” over commutative rings

From here on let us assume that  $R$  is commutative.

The theory of determinants for  $R$  is very similar to the theory of determinants of matrices with entries taken from fields. Given  $A \in M_n(R)$ , the determinant of  $A$  is the value assigned to the list of columns of  $A$  by the unique alternating “multilinear map”  $\varphi : R^n \times \cdots \times R^n \rightarrow R$  such that  $\varphi(\mathbf{e}_1, \dots, \mathbf{e}_n) = 1$ . In other words, we define  $\det(A) = \varphi(\mathbf{a}_1, \dots, \mathbf{a}_n)$  where  $\mathbf{a}_j$  are the columns of  $A$ . Directly by definition, we have  $\det I = 1$ , and the following familiar properties hold because nothing in their usual proofs depends on  $R$  being a field:

$$\det(AB) = \det(A)\det(B), \quad \det(A^t) = \det(A).$$

Let us highlight two properties as exercises:

§22. EXERCISE. Let  $A \in M_n(R)$ , and let  $\mathbf{a}_1, \dots, \mathbf{a}_n$  be the columns of  $A$ . Let also  $\mathbf{b} = r_1\mathbf{a}_1 + \cdots + r_n\mathbf{a}_n$ , and let  $B$  be the matrix that results from replacing column  $j$  of  $A$  by  $\mathbf{b}$ . Prove that

$$\det B = r_j \det A.$$

§23. EXERCISE. Let  $A \in M_n(R)$ , and let  $B$  be the transpose of the matrix of cofactors of  $A$ . Show that

$$AB = BA = (\det A)I,$$

and that, as a consequence,  $A$  is invertible if and only if  $\det A \in R^\times$ , in which case

$$A^{-1} = (\det A)^{-1}B.$$

§24. REMARK. If  $R$  is a field, the condition  $\det(A) \in R^\times$  is equivalent to  $\det(A) \neq 0$ , giving us a well known characterization of invertible matrices in linear algebra.

Let us illustrate an application of the above properties.

§25. PROPOSITION. Let  $\mathbf{a}_1 = (r, 0, \dots, 0) \in R^n$  ( $n \geq 2$ ). Then  $\mathbf{a}_1$  can be part of a basis  $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$  of the free module  $R^n$  if and only if  $r \in R^\times$ .

*Proof.* Assume that  $r \in R^\times$ . Then, letting  $\mathbf{a}_i = \mathbf{e}_i$  for each  $i = 2, \dots, n$ , we obtain a basis because any vector  $(s_1, \dots, s_n)$  is a linear combination of the  $\mathbf{a}_i$ 's with unique coefficients:

$$(s_1, \dots, s_n) = s_1 r^{-1} \mathbf{a}_1 + s_2 \mathbf{a}_2 + \dots + s_n \mathbf{a}_n.$$

Conversely, let us assume that  $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$  is a basis of  $R^n$ , where  $\mathbf{a}_1 = (r, 0, \dots, 0)$  as above. This means that for every vector  $\mathbf{s} = (s_1, \dots, s_n)$  there is a unique vector of coefficients  $\mathbf{x} = (x_1, \dots, x_n)$  such that

$$(s_1, \dots, s_n) = x_1 \mathbf{a}_1 + \dots + x_n \mathbf{a}_n.$$

Or, in matrix form, writing each  $\mathbf{a}_j$  as the  $j$ -column of a matrix  $A$ , we conclude that there is a unique  $\mathbf{x}$  such that

$$\mathbf{s} = A\mathbf{x}.$$

Then, letting successively  $\mathbf{s} = \mathbf{e}_1, \dots, \mathbf{s} = \mathbf{e}_n$ , we obtain a unique  $n \times n$  matrix  $X$  such that

$$I = AX,$$

so  $A$  is invertible, and therefore  $\det A \in R^\times$ . Explicitly, let

$$A = \begin{pmatrix} r & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

and let  $B$  be the  $(n-1) \times (n-1)$  matrix that results from deleting the first row and the first column of  $A$ :

$$B = \begin{pmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Applying the Laplace rule to the first column we obtain

$$\det A = r \det B.$$

Since  $\det A \in R^\times$ , it follows that  $r \in R^\times$  (because, for any commutative unital ring, if  $rs$  has an inverse  $t$  we have  $rst = 1$ , and thus  $r$  has the inverse  $st$  — notice that this reasoning fails for noncommutative rings, for then all we conclude is that  $r$  has a right inverse and  $s$  has a left inverse). ■

## 4 “Linear algebra” over integral domains

From now on  $R$  is an integral domain.

§26. EXAMPLES.  $\mathbb{Z}$  is an integral domain; any field  $F$  is an integral domain, and so is  $F[x]$ .

§27. PROPOSITION. *In an integral domain we have the cancellation law: for all  $r \neq 0$ , if  $ra = rb$  then  $a = b$ .*

*Proof.*  $ra = rb \iff r(a - b) = 0$ , so  $r \neq 0$  implies  $a = b$ . ■

Recall that the construction of the rational numbers from the integers can be mimicked for any integral domain  $R$ . Define an equivalence relation on  $R \times (R \setminus \{0\})$  by

$$(r_1, d_1) \sim (r_2, d_2) \iff r_1 d_2 = r_2 d_1.$$

(Verify that this is an equivalence relation.) The equivalence classes for this equivalence relation are called *fractions*, and the equivalence class of the pair  $(r, d)$  is written as  $r/d$ , or  $\frac{r}{d}$ . Then we must prove that the following two operations are well defined on the fractions (exercise),

$$\frac{r_1}{d_1} \frac{r_2}{d_2} = \frac{r_1 r_2}{d_1 d_2} \quad \text{and} \quad \frac{r_1}{d_1} + \frac{r_2}{d_2} = \frac{r_1 d_2 + r_2 d_1}{d_1 d_2},$$

and that these operations make the set of fractions a unital ring with unit  $\frac{1}{1}$ . Let us denote this ring by  $F$ . Then  $F$  is actually a field, for each nonzero fraction  $\frac{r}{d}$  has the inverse  $\frac{d}{r}$ , and there is an injective unital homomorphism of unital rings

$$i : R \rightarrow F$$

given by  $i(r) = \frac{r}{1}$ , which has the following universal property:

§28. PROPOSITION. *For all injective unital homomorphisms  $f : R \rightarrow F'$  into a field  $F'$  there is a unique (and necessarily injective) homomorphism of unital rings  $f^\# : F \rightarrow F'$  such that  $f^\# \circ i = f$ :*

$$\begin{array}{ccc} R & \xrightarrow{i} & F \\ & \searrow f & \downarrow f^\# \\ & & F' \end{array}$$

*Proof.* Exercise. ■

Hence,  $F$  can be regarded as the “smallest field that contains  $R$ ,” and (as with any universal arrow) it is unique up to an isomorphism. It is the *quotient field* of  $R$ , or the *field of fractions* of  $R$ .

§29. EXERCISE. Let  $C$  be the category whose objects are the integral domains and whose morphisms are the injective unital ring homomorphisms. Similarly, let  $D$  be the category whose objects are the fields and whose morphisms are the injective unital ring homomorphisms. Describe an adjunction from  $C$  to  $D$ .

§30. REMARK. We shall usually regard  $R$  as being a unital subring of its quotient field, by identifying each  $r \in R$  with the fraction  $\frac{r}{1}$ , in the same way that we regard  $\mathbb{Z}$  as a subring of  $\mathbb{Q}$ .

§31. EXERCISE. Prove, for an integral domain  $R$ , that any  $m$  vectors of  $R^n$  with  $m > n$  must be linearly dependent. Hint: begin by considering these to be vectors of the vector space  $F^n$  over  $F$ , where  $F$  is the quotient field of  $R$ .

§32. EXERCISE. Prove, for an integral domain  $R$ , that any basis of the free module  $R^n$  must have exactly  $n$  vectors.

§33. EXERCISE. Prove, for an integral domain  $R$ , that the following conditions on any square matrix  $A \in M_n(R)$  are equivalent:

1. The columns of  $A$  are linearly independent vectors of  $R^n$ .
2. The rows of  $A$  are linearly independent vectors of  $R^n$ .
3.  $\det A \neq 0$ .

§34. COROLLARY. *For any integral domain  $R$ , any invertible matrix  $A \in M_n(R)$  has linearly independent columns.*

*Proof.* The invertibility of  $A$  implies  $\det(A) \in R^\times$ , so  $\det(A) \neq 0$ . Then the result follows from §33. ■

So we see that for integral domains the equivalence, well known in linear algebra, between invertibility of a matrix  $A$  and linear independence of the columns of  $A$  is reduced to only an implication. The following example shows that indeed there is no equivalence in general:

§35. EXAMPLE. Let  $A \in M_n(\mathbb{Z})$  be

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

We have  $\det(A) = 3 \neq 0$ , so the columns are linearly independent, but  $\det(A)$  is not invertible in  $\mathbb{Z}$ , so  $A$  is not invertible in  $M_n(\mathbb{Z})$ . All we can do is to compute  $A^{-1}$  in  $M_n(\mathbb{Q})$ :

$$A^{-1} = \begin{pmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{pmatrix}.$$

## 5 Solutions to some exercises

§36. SOLUTION OF §32. Since, by §31, any set of  $m$  vectors with  $m > n$  must be linearly dependent in  $R^n$ , all we need to show is that no basis can have fewer than  $n$  vectors. Let  $m < n$  and suppose that a set  $A := \{\mathbf{a}_1, \dots, \mathbf{a}_m\}$  is a basis of  $R^n$ . The free module  $F_R(A)$  is isomorphic to  $R^m$ , so we would have an isomorphism  $R^m \cong R^n$  of free modules. Let  $\varphi : R^n \rightarrow R^m$  be such an isomorphism, and let  $E = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$  be the canonical basis of  $R^n$ . Then  $\varphi(E)$  is a linearly independent set of  $n$  vectors of  $R^m$  with  $n > m$ , a contradiction due to §31. ■