Math 332 Winter 2023, Lecture 21: Modules

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

2. Modules

2.5. Spanning, linear independence, bases and free modules (cont'd)

2.5.4. Free modules (cont'd)

Last time, we defined bases of an R-module, and we called an R-module free if it has one. Note that free R-modules of rank n are a natural generalization of vector spaces of dimension n, but not the only possible generalization[1].

Now, let us discuss examples. We begin with examples that make sense for any ring R. We fix an arbitrary ring R.

- Consider the left R-module
$$R^2 = \{(a,b) \mid a,b \in R\}.$$
This R-module R^2 is free of rank 2, since the list
$$((1,0),\ (0,1))$$
is a basis of R^2. Indeed:
  - The vectors $(1,0)$ and $(0,1)$ span R^2, because any vector $(a,b) \in R^2$ can be written as $a(1,0) + b(0,1)$ and thus is a linear combination of $(1,0)$ and $(0,1)$.
  - The vectors $(1,0)$ and $(0,1)$ are linearly independent, since a linear combination $a(1,0) + b(0,1) = (a,b)$ can only equal 0 if $a = b = 0$.
- Likewise, the left R-module R^3 has basis
$$((1,0,0),\ (0,1,0),\ (0,0,1)).$$
- More generally: For any $n \in \mathbb{N}$, the left R-module R^n has basis
$$\begin{pmatrix} (1,0,0,0,\ldots,0), \\ (0,1,0,0,\ldots,0), \\ (0,0,1,0,\ldots,0), \\ \ldots, \\ (0,0,0,0,\ldots,1) \end{pmatrix}.$$

[1] In linear algebra, the dimension of a vector space can be characterized in different ways: e.g., as the size of a basis; as the smallest size of a spanning set; as the largest size of a linearly independent set. If we generalize these three characterizations to an arbitrary ring, they no longer remain equivalent.

This basis is called the **standard basis** of R^n, and its n vectors are called $e_1, e_2, \ldots, e_n$ (in this order). To make this more rigorous: For each $i \in \{1, 2, \ldots, n\}$, we define e_i to be the vector in R^n whose i-th entry is 1 and whose all other entries are 0. Then, the list $(e_1, e_2, \ldots, e_n)$ is a basis of the left R-module R^n. So this R-module is free of rank n.

- In particular, R^1 is free of rank 1. Since $R^1 \cong R$ as left R-modules (because there is an R-module isomorphism $R \to R^1$ that sends each $r \in R$ to the 1-tuple (r)), this entails that R itself is a free R-module of rank 1, with basis (1).

  Also, the R-module R^0 is free of rank 0; here, the empty list serves as a basis (and the only vector in R^0 is also the empty list, by coincidence).

- More generally: If I is a set, then the set

$$R^I = \prod_{i \in I} R = \left\{ (r_i)_{i \in I} \mid \text{all } r_i \text{ belong to } R \right\}$$

  is a left R-module (with entrywise addition and action). If I is finite, this R-module is free (indeed, if I is an n-element set, then R^I is essentially just R^n, except that the vectors are indexed by the elements of I instead of by the numbers $1, 2, \ldots, n$). If I is infinite, the R-module R^I is usually not free. For instance, the $\mathbb{Z}$-module

$$\mathbb{Z}^{\mathbb{N}} = \{\text{all infinite sequences of integers}\}$$

  is not free. (This is fairly tricky to prove! However, you can easily convince yourself that the most obvious candidate for a basis – i.e., the family

$$\begin{array}{l} (\ (1,0,0,0,\ldots), \\ \quad (0,1,0,0,\ldots), \\ \quad (0,0,1,0,\ldots), \\ \quad (0,0,0,1,\ldots), \\ \quad \ldots\ ) \end{array}$$

  – is not a basis, because $(1,1,1,\ldots)$ is not a linear combination of it.[2]) In general, whether $R^{\mathbb{N}}$ is free or not depends on R; in particular, it is free when R is a field (by Theorem 2.5.6 in Lecture 20), but this is not a basis you can construct (or would want to use).

  However, the left R-module R^I has a very important submodule that is free. Namely, let us define a subset $R^{(I)}$ of R^I by

$$\begin{aligned} R^{(I)} &= \left\{ (r_i)_{i \in I} \in R^I \mid \text{all but finitely many } i \in I \text{ satisfy } r_i = 0 \right\} \\ &= \left\{ (r_i)_{i \in I} \in R^I \mid \text{only finitely many } i \in I \text{ satisfy } r_i \neq 0 \right\}. \end{aligned}$$

[2] If this surprises you, recall that linear combinations are not allowed to have infinitely many nonzero coefficients.

For instance,

$$\left(1, 0, 3, \underbrace{0, 0, 0, \ldots}_{\text{only zeroes here}}\right) \in R^{(I)} \qquad \text{but}$$

$$(1, 1, 1, 1, \ldots) \notin R^{(I)} \text{ (unless } R \text{ is trivial).}$$

This subset $R^{(I)}$ is a left R-submodule of R^I (this is not hard to check)[3]. As a left R-module, this $R^{(I)}$ is free; a basis for it is the family $(e_i)_{i \in I}$, where each vector $e_i \in R^{(I)}$ is the vector (i.e., a family indexed by I) whose i-th entry is 1 and whose all other entries are 0. This basis, again, is called the **standard basis** of $R^{(I)}$, and generalizes the standard basis of R^n (because if $I = \{1, 2, \ldots, n\}$, then $R^{(I)} = R^I = R^n$).

- Let R be a ring. Let $n, m \in \mathbb{N}$. Then, the left R-module $R^{n \times m}$ of all $n \times m$-matrices (as defined in §2.1.3 in Lecture 18) is free. It has a basis $\left(E_{i,j}\right)_{(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}}$ consisting of the **elementary matrices** $E_{i,j}$. Each elementary matrix $E_{i,j}$ has a 1 in its (i,j)-th cell and 0s in all other cells. For instance, for $n = 2$ and $m = 3$, this basis consists of the six elementary matrices

$$E_{1,1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad E_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad E_{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$
$$E_{2,1} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad E_{2,2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad E_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

  There are many other bases of $R^{n \times m}$ as well.

- Let $n \in \mathbb{N}$. The set of all symmetric $n \times n$-matrices forms a left R-submodule $R^{n \times n}_{\text{symm}}$ of the left R-module $R^{n \times n}$. It, too, is free. For example, for $n = 2$, it has a basis consisting of the three matrices

$$E_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad E_{1,2} + E_{2,1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad E_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let us now look at $\mathbb{Z}$-modules. As we know from §2.3 (in Lecture 19), these are just abelian groups in fancy clothes, but let us see which of them are free (as $\mathbb{Z}$-modules).

- Consider the $\mathbb{Z}$-submodule

$$U := \left\{(a, b, c) \in \mathbb{Z}^3 \mid a + b + c = 0\right\} \text{ of } \mathbb{Z}^3.$$

[3] Note that $R^{(I)}$ is a straightforward generalization of the R-submodule $R^{(\mathbb{N})}$ constructed in §2.1.3 (Lecture 18).

Is U free? Can we find a basis for U ?

If $\mathbb{Z}$ was a field (like $\mathbb{Q}$ or $\mathbb{R}$), then this would be an instance of a standard problem in linear algebra: You have a homogeneous linear equation (in our case, $a+b+c=0$), and you want to find a basis for its solution space (which is U). There is a standard way to solve such a problem (see, e.g., [LaNaSc16, §A.3.2]) Use Gaussian elimination to bring the matrix of the equations into row echelon form, and use the latter to write down a basis (using free and bound variables). However, Gaussian elimination relies crucially on the possibility of dividing by a nonzero scalar. We can do this over a field, but not over $\mathbb{Z}$.

The good news is that in the specific case of U, no division is needed (since our matrix $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$ has only one row, and this row starts with a 1). Thus, Gaussian elimination does work here, and produces the basis

$$((-1,0,1),\ \ (0,-1,1)).$$

You can check directly that this is a basis[4].

Alternatively, there are many other bases, such as

$$((1,-1,0),\ \ (0,1,-1)).$$

Either way, you find that U is free of rank 2.

What happens for $\mathbb{Z}$-submodules of $\mathbb{Z}^n$ given by more complicated systems of linear equations? Are they still free? Yes, but this requires a more sophisticated algorithm than Gaussian elimination. See §7.1 in the text for this.

[4]Here is the straightforward verification:

- Each vector in U has the form $(a,b,c) \in \mathbb{Z}^3$ with $a+b+c=0$, and thus can be rewritten as

$$\begin{aligned}(a,b,c) &= (a,b,-a-b) && \text{(since } a+b+c=0 \text{ entails } c=-a-b\text{)}\\ &= a\,(1,0,-1) + b\,(0,1,-1)\\ &= (-a)\,(-1,0,1) + (-b)\,(0,-1,1),\end{aligned}$$

  which is visibly a $\mathbb{Z}$-linear combination of $(-1,0,1)$ and $(0,-1,1)$. Thus, the vectors $(-1,0,1)$ and $(0,-1,1)$ span U.

- These two vectors are furthermore $\mathbb{Z}$-linearly independent, because if a linear combination $a\,(-1,0,1) + b\,(0,-1,1)$ is 0, then

$$\begin{aligned}a\,(-1,0,1) + b\,(0,-1,1) = 0 = (0,0,0), &\qquad \text{thus}\\ (-a,-b,a+b) = (0,0,0), &\qquad \text{thus}\\ -a = -b = a+b = 0, &\qquad \text{thus}\\ a = b = 0.\end{aligned}$$

- The $\mathbb{Z}$-module $\mathbb{Z}/2$ is not free. More generally: Any free $\mathbb{Z}$-module is either trivial or infinite; thus, a nontrivial finite abelian group can never be free as a $\mathbb{Z}$-module.
- The $\mathbb{Z}$-module $\mathbb{Q}$ is not free. In a nutshell, this is because 1 vector is not enough to span $\mathbb{Q}$, but 2 vectors already fail to be linearly independent. (See §3.7.3 in the text for details.)
- Now, consider the $\mathbb{Z}$-submodule

$$V := \left\{ (a,b) \in \mathbb{Z}^2 \mid a \equiv b \bmod 2 \right\} \text{ of } \mathbb{Z}^2.$$

  This $\mathbb{Z}$-submodule V contains the vectors $(0,2)$ and $(1,1)$ and $(1,-1)$ and $(4,-2)$ and many others. Is V free? Can we find a basis for it?

  We can start with the list $((2,0),\ (0,2))$. This list is linearly independent (why?), but does not span V (why not?), so is not a basis.

  How can we fix this? We can try inserting a new vector into our list, say $(1,1)$. Thus, we get a list $((2,0),\ (0,2),\ (1,1))$, which spans V (why?), but is no longer linearly independent (why not?), so again is not a basis.

  But let us now remove the vector $(0,2)$ from our list. So we end up with the list $((2,0),\ (1,1))$. This list is linearly independent, because if a linear combination $a\,(2,0) + b\,(1,1)$ is 0, then we find

$$\begin{aligned} &a\,(2,0) + b\,(1,1) = 0, && \text{thus} \\ &(2a+b,\ b) = 0, && \text{thus} \\ &2a + b = 0 \text{ and } b = 0, && \text{thus} \\ &a = b = 0. \end{aligned}$$

  Furthermore, this list $((2,0),\ (1,1))$ spans V, because if (a,b) is any vector in V (that is, any vector in $\mathbb{Z}^2$ that satisfies $a \equiv b \bmod 2$), then

$$(a,b) = \underbrace{\frac{a-b}{2}}_{\substack{\in \mathbb{Z} \\ (\text{since } a \equiv b \bmod 2)}} (2,0) + b\,(1,1).$$

  Thus, this list $((2,0),\ (1,1))$ is a basis of the $\mathbb{Z}$-module V, so that V is free of rank 2. Other bases of V can easily be found (for example, $((1,1),\ (1,-1))$).
- More examples can be found in §3.7.3 in the text.

Now, let us return to the general case to state a few theorems:

Theorem 2.5.7. Let M be a left R-module. Let $n \in \mathbb{N}$. The left R-module M is free of rank n if and only if $M \cong R^n$ (as left R-modules).

More concretely, a basis of M that consists of n vectors will always produce an isomorphism from R^n to M according to the following method:

Theorem 2.5.8. Let M be a left R-module. Let $m_1, m_2, \ldots, m_n$ be n vectors in M. Consider the map

$$f : R^n \to M,$$
$$(r_1, r_2, \ldots, r_n) \mapsto r_1 m_1 + r_2 m_2 + \cdots + r_n m_n.$$

Then:
(a) This map f is always a left R-module morphism.
(b) This map f is injective if and only if $m_1, m_2, \ldots, m_n$ are linearly independent.
(c) This map f is surjective if and only if $m_1, m_2, \ldots, m_n$ span M.
(d) This map f is an isomorphism (of left R-modules) if and only if $(m_1, m_2, \ldots, m_n)$ is a basis of M.

This can be generalized from R^n to $R^{(I)}$ for arbitrary sets I:

Theorem 2.5.9. Let M be a left R-module. Let $(m_i)_{i \in I}$ be a family of vectors in M. Consider the map

$$f : R^{(I)} \to M,$$
$$(r_i)_{i \in I} \mapsto \sum_{i \in I} r_i m_i.$$

(This is well-defined, because $(r_i)_{i \in I} \in R^{(I)}$ ensures that the sum $\sum_{i \in I} r_i m_i$ has only finitely many nonzero addends.)
Then:
(a) This map f is always a left R-module morphism.
(b) This map f is injective if and only if $(m_i)_{i \in I}$ is linearly independent.
(c) This map f is surjective if and only if $(m_i)_{i \in I}$ spans M.
(d) This map f is an isomorphism (of left R-modules) if and only if $(m_i)_{i \in I}$ is a basis of M.

Proofs of these three theorems can be found in §3.7.3 of the text. None of them is hard.

Remark 2.5.10. Can a left R-module be free of two different ranks at the same time? In other words, can R^n be isomorphic to R^m as left R-modules for two different integers n and m?

The answer is "yes" for a stupid reason: If R is a trivial ring, then any R-module is free of any rank (and is trivial), and we have $R^0 \cong R^1 \cong R^2 \cong \cdots$.

If we ignore trivial rings for a moment, the answer is still "yes": For instance, [DumFoo04, §10.3, exercise 27] constructs a ring R over which $R^n \cong R$ as left R-modules for each $n \in \{1, 2, 3, \ldots\}$ (so that R itself is a free R-module of rank n for each $n \in \{1, 2, 3, \ldots\}$).

However, if R is a **nontrivial commutative** ring, then the answer is "no". In this case, the R-modules $R^0, R^1, R^2, \ldots$ are mutually non-isomorphic, so that a free R-module can never have two different ranks at the same time. This is not obvious at all (see [DumFoo04, §10.3, exercise 2]). We can actually say more: If R is a nontrivial commutative ring, then an R-module morphism $R^m \to R^n$ cannot be injective unless $m \leq n$ (see, e.g., `https://math.stackexchange.com/questions/106786`), and cannot be surjective unless $m \geq n$ (see, e.g., `https://math.stackexchange.com/questions/20178`). These facts are in line with the intuition you should have from linear algebra (injective maps cannot quash dimensions; surjective maps cannot create dimensions) and also with the Pigeonhole Principles from combinatorics (a map between two finite sets M and N cannot be injective unless $|M| \leq |N|$, and cannot be surjective unless $|M| \geq |N|$). But actually proving them takes real work.

2.6. The universal property of a free module

As before, fix a ring R.

Recall that R-linear maps (that is, R-module morphisms) respect addition, scaling and zero. Thus, they also respect linear combinations (in the sense that if you apply a linear map to a linear combination of some vectors, then you get the analogous linear combination of their images):

Proposition 2.6.1. Let M and P be two left R-modules. Let $f : M \to P$ be an R-linear map. Let $(m_i)_{i \in I}$ be a family of vectors in M, and let $(r_i)_{i \in I} \in R^{(I)}$ be a family of scalars. Then,

$$f\left(\sum_{i \in I} r_i m_i\right) = \sum_{i \in I} r_i f\left(m_i\right).$$

Proof. This is easy if the set I is finite. For example, if $I = \{1, 2, 3\}$, then this is saying that

$$f\left(r_1 m_1 + r_2 m_2 + r_3 m_3\right) = r_1 f\left(m_1\right) + r_2 f\left(m_2\right) + r_3 f\left(m_3\right),$$

and this can be proved as follows:

$$\begin{aligned}
&f\left(r_1m_1 + r_2m_2 + r_3m_3\right) \\
&= f\left(r_1m_1\right) + f\left(r_2m_2 + r_3m_3\right) && \text{(since } f \text{ respects addition)} \\
&= f\left(r_1m_1\right) + f\left(r_2m_2\right) + f\left(r_3m_3\right) && \text{(since } f \text{ respects addition)} \\
&= r_1f\left(m_1\right) + r_2f\left(m_2\right) + r_3f\left(m_3\right) && \text{(since } f \text{ respects scaling)}\,.
\end{aligned}$$

The case of an arbitrary finite set I is similar (for a rigorous proof, induct on $|I|$).

The general case (i.e., when I is not necessarily finite) can be reduced to the finite case by observing that only finitely many $i \in I$ satisfy $r_i \neq 0$ (since $(r_i)_{i\in I} \in R^{(I)}$). See the proof of Proposition 3.8.1 in the text for details. □

Now we shall state the **universal property of free modules**. This property provides an easy way to construct linear maps out of free modules (just like the universal property of quotient rings provides an easy way to construct ring morphisms out of quotient rings). Indeed, if M is a module with a basis $(m_i)_{i\in I}$, and you want to define a linear map f out of M, then it suffices to specify the values $f\left(m_i\right)$ of the map on each vector of the basis. These values can be specified arbitrarily; each possible specification yields a unique linear map f. The universal property of free modules is just putting this in formal words:

Theorem 2.6.2 (Universal property of free modules)**.** Let M be a free left R-module with basis $(m_i)_{i\in I}$. Let P be a further left R-module (free or not). Let $p_i \in P$ be a vector for each $i \in I$. Then, there exists a **unique** R-linear map $f : M \to P$ such that

$$\text{each } i \in I \text{ satisfies } f\left(m_i\right) = p_i. \tag{1}$$

Explicitly, this map is given by

$$f\left(\sum_{i\in I} r_i m_i\right) = \sum_{i\in I} r_i p_i \qquad \text{for all } (r_i)_{i\in I} \in R^{(I)}. \tag{2}$$

This theorem says that if you want to construct a linear map f out of a free R-module M with a given basis $(m_i)_{i\in I}$, you only need to specify the images $f\left(m_i\right)$ of the basis vectors m_i. Once you have specified those images, the linearity of f will automatically determine all other values of f, thus defining the map uniquely.

For instance, recall that the R-module R^3 has standard basis (e_1, e_2, e_3). Thus, if you want to construct a linear map f from R^3 to another R-module P, you only need to specify $f\left(e_1\right)$, $f\left(e_2\right)$, $f\left(e_3\right)$. Once you have done this, the linearity of f will ensure that

$$f\left(r_1e_1 + r_2e_2 + r_3e_3\right) = r_1f\left(e_1\right) + r_2f\left(e_2\right) + r_3f\left(e_3\right) \qquad \text{for all } r_1, r_2, r_3 \in R,$$

and this uniquely determines f because any vector in R^3 can be uniquely written as a linear combination $r_1e_1 + r_2e_2 + r_3e_3$ of e_1, e_2, e_3.

Proof of Theorem 2.6.2. The family $(m_i)_{i\in I}$ is a basis of M. Thus, by Proposition 2.5.4 **(c)** in Lecture 20, we know that each vector $v \in M$ can be written as an R-linear combination of $(m_i)_{i\in I}$ in **exactly one** way. In other words, each $v \in M$ can be written in the form $v = \sum_{i\in I} r_i m_i$ for a **unique** family $(r_i)_{i\in I} \in R^{(I)}$ of scalars. Thus, the equality (2) uniquely defines a map $f : M \to P$. Furthermore, the map f defined by this equality is easily seen to be R-linear and to satisfy $f(m_i) = p_i$ for each $i \in I$. Thus, we have proved that there exists an R-linear map $f : M \to P$ that satisfies (1), and that this map is explicitly given by (2).

It remains to show that this map is the **only** R-linear map $f : M \to P$ that satisfies (1). But this is again easy: If $f : M \to P$ is any R-linear map satisfying (1), then Proposition 2.6.1 yields

$$f\left(\sum_{i\in I} r_i m_i\right) = \sum_{i\in I} r_i \underbrace{f(m_i)}_{\substack{=p_i \\ \text{(by (1))}}} = \sum_{i\in I} r_i p_i \qquad \text{for all } (r_i)_{i\in I} \in R^{(I)},$$

and thus our map f must be identical to the map f defined by (2). Thus, uniqueness follows. This completes the proof of Theorem 2.6.2. □

We note that the uniqueness part of Theorem 2.6.2 (i.e., the part claiming that f is unique) is true under a weaker assumption: It suffices to require that the family $(m_i)_{i\in I}$ spans M (as opposed to being a basis of M). This is a useful (if easy) fact, so we state it as a theorem:

Theorem 2.6.3 (Linear maps are determined on a spanning set)**.** Let M be a left R-module. Let $(m_i)_{i\in I}$ be a family of vectors in M that spans M. Let P be a further left R-module. Let $f, g : M \to P$ be two R-linear maps such that

$$\text{each } i \in I \text{ satisfies } f(m_i) = g(m_i).$$

Then, $f = g$.

This theorem is often used to prove that two linear maps are equal.

Proof of Theorem 2.6.3. Let $v \in M$. Then, v can be written as an R-linear combination of $(m_i)_{i\in I}$ (since the family $(m_i)_{i\in I}$ spans M). In other words, $v = \sum_{i\in I} r_i m_i$ for some family $(r_i)_{i\in I} \in R^{(I)}$ of scalars. Consider this family. Now, from $v = \sum_{i\in I} r_i m_i$, we obtain

$$f(v) = f\left(\sum_{i\in I} r_i m_i\right) = \sum_{i\in I} r_i f(m_i) \qquad \text{(by Proposition 2.6.1)}$$

and similarly

$$g(v) = \sum_{i \in I} r_i g(m_i).$$

The right hand sides of these two equalities are equal (since we assumed that each $i \in I$ satisfies $f(m_i) = g(m_i)$). Hence, their left hand sides must be equal as well. In other words, $f(v) = g(v)$. Since we have proved this for every $v \in M$, we thus conclude that $f = g$. □

References

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.
See `https://site.uvm.edu/rfoote/files/2022/06/errata_3rd_edition.pdf` for errata.

[LaNaSc16] Isaiah Lankham, Bruno Nachtergaele, Anne Schilling, *Linear Algebra As an Introduction to Abstract Mathematics*, 2016.
`https://www.math.ucdavis.edu/~anne/linear_algebra/mat67_course_notes.pdf`