Math 332 Winter 2023, Lecture 18: Modules

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

2. Modules

So far, we have been studying rings. Now we shall move on to studying modules over these rings.

Roughly speaking, a ring is a system of "number-like objects" that can be "added" (with one another) and "multiplied" (with one another).

In contrast, a **module** (over a given ring R) is a system of "vector-like objects" that can be "added" (with one another) and "scaled" (by elements of R). If this sounds familiar to you, then you are right: Modules generalize vector spaces. In many ways, modules are simpler and better-behaved than rings; but of course, they rely on rings, whence we have had to introduce rings before introducing modules.

2.1. Definitions and examples

Convention 2.1.1. We shall fix a ring R for the rest of this section.

2.1.1. Defining modules

There are two notions of an "R-module": the "left R-modules" and the "right R-modules". Let us define the left ones:

Definition 2.1.2. Let R be a ring. A **left R-module** (or a **left module over** R) means a set M equipped with

- a binary operation $+$ (that is, a map from $M \times M$ to M) that is called **addition**;
- an element 0_M of M that is called the **zero element** or the **zero vector** or just the **zero**, and will be just denoted by 0 if there is no danger of confusion;
- a map from $R \times M$ to M that is called the **action of R on** M, and is written as multiplication (i.e., we denote the image of a pair $(r, m) \in R \times M$ under this map by rm or $r \cdot m$)

such that the following properties (the "**module axioms**") hold:

- $(M, +, 0)$ is an abelian group.
- The **right distributivity law** holds: We have $(r + s)\, m = rm + sm$ for all $r, s \in R$ and $m \in M$.

- The **left distributivity law** holds: We have $r(m+n) = rm + rn$ for all $r \in R$ and $m, n \in M$.
- The **associativity law** holds: We have $(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$.
- We have $0_R m = 0_M$ for every $m \in M$.
- We have $r \cdot 0_M = 0_M$ for every $r \in R$.
- We have $1m = m$ for every $m \in M$.

When M is a left R-module, the elements of M are called **vectors**, and the elements of R are called **scalars**.

As the name "left R-module" suggests, there is an analogous notion of a **right R-module**. In this latter notion, the action is not a map from $R \times M$ to M but a map from $M \times R$ to M, and we accordingly use the notation mr rather than rm for its values. The associativity law for right R-modules requires that $m(rs) = (mr)s$ for all $r, s \in R$ and $m \in M$.

When the ring R is commutative, any left R-module M becomes a right R-module by setting

$$mr = rm \qquad \text{for all } r \in R \text{ and } m \in M,$$

and conversely, any right R-module M becomes a left R-module by setting

$$rm = mr \qquad \text{for all } r \in R \text{ and } m \in M.$$

In other words, when the ring R is commutative, we can "translate" any left action[1] of R on M into a right action, and vice versa.

This mutual "translatability" allows us to treat left R-modules and right R-modules as the same thing when R is a commutative ring. Thus, when R is commutative, we will just speak of "**R-modules**" and view them as left or right as we please.

However, if R is not commutative, then our "translation" between left and right R-modules will usually destroy associativity: For example, if M is a left R-module, then its associativity law says that $(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$. If we translate its left action into a right action, then this equality becomes $m(rs) = (ms)r$, which is **not** the associativity law for a right R-module. There is a way to salvage this using the **opposite ring** R^{op} of R; this is the same ring as R but with the order of multiplication swapped (i.e., what is rs in R becomes sr in R^{op}). Then, a left R-module becomes a right R^{op}-module,

[1] By a "left action", I mean an action of the form $R \times M \to M$, as in the definition of a left R-module. Correspondingly, a "right action" means an action of the form $M \times R \to M$, as in the definition of a right R-module.

and vice versa. (See [21w, homework set #2, Exercise 2 **(d)**] for the details.) Thus, the notion of a left R-module is not equivalent to the notion of a right R-module for a **given** noncommutative ring R, but the general notion of a "left module over a ring" is equivalent to the general notion of a "right module over a ring".

This allows us to focus on left R-modules and sleep well knowing that everything we prove about them has analogue for right R-modules (and the latter can be proved in the same way as the former).

When R is a field, the R-modules are known as the **R-vector spaces**. These are precisely the vector spaces you have seen in an advanced linear algebra class. Vector spaces have a fairly rigid structure: In particular, a vector space is uniquely determined (up to isomorphism) by its dimension. In contrast, modules can be rather wild (although the "nice" families of modules, such as R^n for all $n \in \mathbb{N}$, still exist for every ring R). The wilder the ring is, the more diverse are its modules.

One more remark about Definition 2.1.2: The "$0_R m = 0_M$" and "$r \cdot 0_M = 0_M$" axioms are redundant (i.e., follow from the other axioms). Do you see why?

Another piece of terminology:

Definition 2.1.3. Let M be a left R-module, and let $r \in R$ be a scalar. Then, the map

$$\begin{aligned} M &\to M, \\ m &\mapsto rm \end{aligned}$$

is called **scaling** by r. This map is a group homomorphism from the additive group $(M, +, 0)$ to itself. For instance, scaling by 1 is the identity map on M, whereas scaling by 0 sends every vector in M to the zero vector.

2.1.2. Defining submodules

We will soon see some examples of R-modules; but let us first define R-submodules. This is just the natural generalization of vector subspaces:

Definition 2.1.4. Let M be a left R-module. An **R-submodule** (or, to be more precise, a **left R-submodule**) of M means a subset N of M such that

- we have $a + b \in N$ for all $a, b \in N$ (that is, N is **closed under addition**);
- we have $ra \in N$ for all $r \in R$ and $a \in N$ (that is, N is **closed under scaling**);
- we have $0_M \in N$ (that is, N **contains zero**).

In §2.2.1 (in Lecture 19), we will see that any R-submodule of a left R-module M is also closed under negation (i.e., under taking additive inverses), and thus becomes a left R-module in its own right.[2] Of course, all of this applies likewise to right R-modules.

2.1.3. Examples

Some examples:

- Let R be a ring. Then, R itself becomes a left R-module: Just define the action to be the multiplication of R. Thus, the elements of R serve as both vectors and scalars. Scaling a vector m by a scalar r just means multiplying m by r (that is, taking the product rm inside R).

  The R-submodules of this left R-module R are the subsets L of R that are closed under addition and contain 0 and satisfy $ra \in L$ for all $r \in R$ and $a \in L$. These subsets L are called the **left ideals** of R. They differ from the ideals of R in that we only require $ra \in L$, not $ar \in L$. Correspondingly, many rings have more left ideals than ideals. For example: If R is the matrix ring $\mathbb{Q}^{2\times 2}$, then R has only two ideals ($\{0_R\}$ and R) but plenty of left ideals (e.g., the set $\left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$).

  When R is commutative, the left ideals of R are precisely the ideals of R, so the notion of R-submodules then becomes a generalization of ideals.

- Let R be any ring, and let $n \in \mathbb{N}$. Then,

  $$R^n = \{(a_1, a_2, \ldots, a_n) \mid \text{all } a_i \text{ belong to } R\}$$

  is a left R-module, where addition and action are defined entrywise, i.e., by setting

  $$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1,\ a_2 + b_2,\ \ldots,\ a_n + b_n)$$

  and

  $$r \cdot (a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n) \qquad (\text{for } r \in R).$$

  The zero vector of this R-module is $(0, 0, \ldots, 0)$.

- Let R be any ring, and let $n, m \in \mathbb{N}$. Consider the set $R^{n\times m}$ of all $n \times m$-matrices with entries in R. This set $R^{n\times m}$ is not a ring unless $n = m$, but it always is a left R-module, where addition and action are defined entrywise. For instance, the action is given for 2×2-matrices by

  $$r \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix} \qquad (\text{for } r \in R),$$

[2] Proving this is actually an easy exercise you can solve right now.

and similarly for matrices of all other sizes. The zero vector of $R^{n\times m}$ is the zero matrix $0_{n\times m}$.

This set $R^{n\times m}$ is also a right R-module in a similarly obvious way.

According to Definition 2.1.2, this allows us to refer to the matrices in $R^{n\times m}$ as "vectors". This shows that our notion of vectors is much more general than just row vectors and column vectors. Numbers are vectors; matrices are vectors; everything that lives in a module is a vector. This general interpretation of the word "vector" will soon reveal its usefulness, as it allows us to apply various linear-algebraic notions (such as span and linear independence) to anything that looks, swims and quacks like a vector.

- Just as we defined the left R-module R^n (consisting of n-tuples) for any $n \in \mathbb{N}$, we can define a left R-module "R^∞" consisting of all infinite sequences of elements of R. The proper name of this R-module is $R^{\mathbb{N}}$ (since "∞" is imprecise: there are many infinities in mathematics). Explicitly, $R^{\mathbb{N}}$ is defined to be the left R-module

  $$\{(a_0, a_1, a_2, \ldots) \mid \text{all } a_i \text{ belong to } R\},$$

  whose addition and action are defined entrywise.

  This left R-module $R^{\mathbb{N}}$ has an R-submodule

  $$R^{(\mathbb{N})} := \left\{(a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \mid \text{only finitely many } i \in \mathbb{N} \text{ satisfy } a_i \neq 0\right\}.$$

  You can check that this is indeed an R-submodule of $R^{\mathbb{N}}$. For instance, for $R = \mathbb{Q}$, we have

  $$\begin{aligned}
  (1,1,1,\ldots) &\in R^{\mathbb{N}} \setminus R^{(\mathbb{N})};\\
  (0,0,0,\ldots) &\in R^{(\mathbb{N})};\\
  \Big(3,2,0,5,\underbrace{0,0,0,0,0,\ldots}_{\text{only zeroes here}}\Big) &\in R^{(\mathbb{N})};\\
  \Big(\underbrace{1,0,1,0,1,0,\ldots}_{\text{ones and zeroes alternate}}\Big) &\in R^{\mathbb{N}} \setminus R^{(\mathbb{N})}.
  \end{aligned}$$

Note that the zero vector of an R-module is uniquely determined by its addition, so we don't have to provide it in a definition.

2.1.4. Direct products

Fix a ring R.

Most of our above examples of R-modules involve tuples on which addition and action work entrywise. There is a general concept for this:

Definition 2.1.5. Let $n \in \mathbb{N}$, and let $M_1, M_2, \ldots, M_n$ be any n left R-modules. Then, the Cartesian product $M_1 \times M_2 \times \cdots \times M_n$ becomes a left R-module as well, where addition and action are defined entrywise: e.g., the action is defined by

$$r \cdot (m_1, m_2, \ldots, m_n) = (rm_1, rm_2, \ldots, rm_n) \text{ for all } r \in R \text{ and } m_i \in M_i.$$

This left R-module $M_1 \times M_2 \times \cdots \times M_n$ is called the **direct product** of $M_1, M_2, \ldots, M_n$.

This notion of direct product can be generalized further to direct products of arbitrarily (not necessarily finitely) many left R-modules. The resulting products are called $\prod_{i \in I} M_i$. See §3.3.1 in the text for more about those.

A particular case of direct products is of particular importance:

Definition 2.1.6. Let M be any left R-module. Let $n \in \mathbb{N}$. Then, we set

$$M^n := \underbrace{M \times M \times \cdots \times M}_{n \text{ times}}.$$

In particular, when M is the natural left R-module R (that is, the R-module R whose action is just multiplication), then M^n is the left R-module R^n that was discussed above.

2.1.5. Restriction of scalars

Here are some more ways to construct modules:

- If R is a subring of a ring S, then S is a left R-module (where the action of R on S is defined by restricting the multiplication map $S \times S \to S$ to $R \times S$) and a right R-module (in a similar way).

  Let me restate this in a more down-to-earth way: If R is a subring of a ring S, then we can multiply any element of R with any element of S (since both elements lie in the ring S); this makes S into a left R-module (and likewise, S becomes a right R-module). Explicitly, the action of R on the left R-module S is given by

  $$rs = rs \qquad \text{for all } r \in R \text{ and } s \in S$$

  (where the "rs" on the left hand side means the image of (r, s) under the action, whereas the "rs" on the right hand side means the product of r and s in the ring S).

  Thus, for example, $\mathbb{C}$ is an $\mathbb{R}$-module (since $\mathbb{R}$ is a subring of $\mathbb{C}$) and also a $\mathbb{Q}$-module (for similar reasons). In a linear algebra class, you would say "vector space" instead of "module" here, but this is the same thing.

- More generally, if R and S are any two rings, and if $f : R \to S$ is a ring morphism, then S becomes a left R-module, with the action of R on S being defined by

$$rs = f(r) \cdot s \qquad \text{for all } r \in R \text{ and } s \in S.$$

  In a similar way, S becomes a right R-module (with action defined by $sr = s \cdot f(r)$). This is easy to prove (the module axioms follow from the fact that f is a ring morphism). These R-module structures on S are said to be **induced** by the morphism f.

  Our previous example (where R is a subring of S) is the particular case of this where f is the canonical inclusion[3] (i.e., the map $R \to S,\ r \mapsto r$).

  Here are some other particular cases:

  - Any quotient ring R/I of a ring R (by some ideal I) becomes a left R-module, because the canonical projection $\pi : R \to R/I$ is a ring morphism. Explicitly, the action of R on R/I is given by

$$r \cdot \overline{u} = \underbrace{\pi(r)}_{=\overline{r}} \cdot \overline{u} = \overline{r} \cdot \overline{u} = \overline{ru} \qquad \text{for any } r, u \in R.$$

  - Another (less transparent) particular case: I claim that the abelian group $\mathbb{Z}/5$ becomes a $\mathbb{Z}[i]$-module if we define the action by

$$(a+bi) \cdot m = \overline{a+2b} \cdot m \qquad \text{for all } a+bi \in \mathbb{Z}[i] \text{ and } m \in \mathbb{Z}/5.$$

    This $\mathbb{Z}[i]$-module structure is actually induced by the ring morphism

$$f : \mathbb{Z}[i] \to \mathbb{Z}/5,$$
$$a+bi \mapsto \overline{a+2b},$$

    which is a ring morphism thanks to the fact that $\overline{2}^2 = -\overline{1}$ in $\mathbb{Z}/5$ (check this!). There is also another $\mathbb{Z}[i]$-module structure on $\mathbb{Z}/5$, given by

$$(a+bi) \cdot m = \overline{a+3b} \cdot m \qquad \text{for all } a+bi \in \mathbb{Z}[i] \text{ and } m \in \mathbb{Z}/5.$$

---

[3]Recall what "canonical inclusion" means:

If U is a subset of a set V, then the map

$$U \to V,$$
$$u \mapsto u$$

is called the **canonical inclusion** of U into V.

If U is a subring of a ring V, then the canonical inclusion of U into V is furthermore a ring morphism. (This follows trivially from the definition of a subring.)

When we speak of the $\mathbb{Z}[i]$-module $\mathbb{Z}/5$, we have to specify which of these two structures we are meaning. They are not the same: One structure has $i \cdot \overline{1} = \overline{2}$; the other has $i \cdot \overline{1} = \overline{3}$. So to speak, $\mathbb{Z}/5$ is "a $\mathbb{Z}[i]$-module in two different ways".

- Even more generally: If R and S are two rings, and if $f : R \to S$ is a ring morphism, then any left S-module M (not just S itself) naturally becomes a left R-module, with the action defined by

$$rm = f(r)\, m \qquad \text{for all } r \in R \text{ and } m \in M.$$

  (You can think of this as letting R act on M "by proxy": In order to scale a vector $m \in M$ by a scalar $r \in R$, you just scale it by the scalar $f(r) \in S$.)

  This method of turning S-modules into R-modules is called **restriction of scalars** (or, more specifically, **restricting** an S-module to R via f).

  If we apply this method to a canonical inclusion (i.e., if R is a subring of S and if $f : R \to S$ is the canonical inclusion), then we conclude that any module over a ring naturally becomes a module over any subring.[4] For example, any $\mathbb{C}$-module naturally becomes an $\mathbb{R}$-module (this is known as "decomplexification" in linear algebra) and a $\mathbb{Q}$-module and a $\mathbb{Z}$-module.

References

[21w] Darij Grinberg, *Math 533: Abstract Algebra I, Winter 2021*.
`https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

[4] You can think of it as forgetting how to scale vectors by scalars that don't belong to the subring.