Math 332 Winter 2023, Lecture 19: Modules

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

2. Modules

2.2. A couple generalities

Let us now show a few general properties of modules. Again, we fix a ring R.

2.2.1. Negation and subtraction

We begin with a study of negation (i.e., additive inverses).

Proposition 2.2.1. Let R be a ring. Let M be a left R-module. Then, $(-1)\,a = -a$ for each $a \in M$. (Here, -1 denotes -1_R.)

Proof. Let $a \in M$. Then, $1a = a$ (by one of the module axioms). Thus,

$$\begin{aligned} (-1)\,a + \underbrace{a}_{=1a} &= (-1)\,a + 1a \\ &= \underbrace{((-1)+1)}_{=0_R} a \qquad \text{(by the right distributivity axiom)} \\ &= 0_R a = 0_M \qquad \text{(by one of the module axioms)}. \end{aligned}$$

In other words, $(-1)\,a$ is an additive inverse of a. But the additive inverse of a is $-a$. Thus, we conclude that $(-1)\,a = -a$. This proves Proposition 2.2.1. □

Further properties of negation and scaling can easily be derived from this. For example:

Proposition 2.2.2. Let R be a ring. Let M be a left R-module. Let $r \in R$ and $m \in M$. Then,

$$(-r)\,m = -(rm) = r\,(-m) \tag{1}$$

and

$$(-r)\,(-m) = rm. \tag{2}$$

Proof. Left to the reader. (Just as in the proof of Proposition 2.2.1, argue that both $(-r)\,m$ and $r\,(-m)$ are additive inverses of rm. This proves (1). To get (2), apply (1) to $-m$ instead of m.) □

Proposition 2.2.3. Let R be a ring. Let M be a left R-module. Then, any R-submodule of M is a subgroup of the additive group $(M,+,0)$.

Proof of Proposition 2.2.3. Let N be an R-submodule of M. Then, N is closed under addition and under scaling and contains the zero vector. Each $a \in N$ satisfies

$$\begin{aligned} -a &= (-1)\, a && \text{(by Proposition 2.2.1)} \\ &\in N && \text{(since } N \text{ is closed under scaling)}. \end{aligned}$$

In other words, N is closed under negation (= taking additive inverses). Thus, N is a subgroup of $(M, +, 0)$. □

Proposition 2.2.4. Let R be a ring. Let M be a left R-module. Then, an R-submodule of M is the same as a subgroup of the additive group $(M, +, 0)$ that is closed under scaling by every scalar $r \in R$.

Proof. Any R-submodule of M is a subgroup of the additive group $(M, +, 0)$ (by Proposition 2.2.3) that is closed under scaling by every scalar $r \in R$ (by the definition of a submodule). Conversely, any subgroup of the additive group $(M, +, 0)$ that is closed under scaling by every scalar $r \in R$ is an R-submodule of M (since it satisfies all the axioms for a submodule). Thus, Proposition 2.2.4. □

Proposition 2.2.5. Let R be a ring. Let M be a left R-module. Then, any R-submodule of M becomes a left R-module in its own right (just like a subring of a ring becomes a ring).

Proof. Let N be an R-submodule of M. Then, Proposition 2.2.3 shows that N is a subgroup of the additive group $(M, +, 0)$. Hence, $(N, +, 0)$ is a group. Since N is closed under scaling, we can also define an action of R on N in the obvious way (viz., inheriting it from M). This makes N into a left R-module. This proves Proposition 2.2.5. □

We also have "distributivity laws for subtraction":

Proposition 2.2.6. Let R be a ring. Let M be a left R-module. Then:
(a) We have $(r - s)\, m = rm - sm$ for all $r, s \in R$ and $m \in M$.
(b) We have $r\,(m - n) = rm - rn$ for all $r \in R$ and $m, n \in M$.

Proof. LTTR. (The fastest way is to derive these properties from the distributivity laws by strategic application of (1).) □

2.2.2. Finite sums

Finite sums $\sum\limits_{s \in S} a_s$ of elements of an R-module are defined just as they are in a ring. Finite products, of course, cannot be defined, since an R-module does not have any internal multiplication.

The generalized distributivity laws

$$(r_1 + r_2 + \cdots + r_n)\, a = r_1 a + r_2 a + \cdots + r_n a \qquad \text{and}$$
$$r\,(a_1 + a_2 + \cdots + a_n) = r a_1 + r a_2 + \cdots + r a_n$$

hold in every left R-module A (for any $r, r_1, r_2, \ldots, r_n \in R$ and any $a, a_1, a_2, \ldots, a_n \in A$).

Convention 2.2.7. Let R be a ring. Let M be a left R-module. Let $r, s \in R$ and $m \in M$. Since $(rs)\, m$ and $r\,(sm)$ are the same element of M (by associativity), we will just denote them by rsm without parentheses.

2.2.3. Principal submodules

Here is a particularly easy way to construct submodules:

Proposition 2.2.8. Let R be a ring. Let a be a central element of R (that is, an element of R that commutes with all elements of R). Let M be a left R-module. Then,

$$aM := \{am \mid m \in M\}$$

is an R-submodule of M.

In particular, $0M = \{0_M\}$ and $1M = M$ are R-submodules of M.

Proof. LTTR. (Note that this generalizes the construction of principal ideals in R.) □

Clearly, any R-submodule N of M lies between $0M$ and $1M$ (that is, satisfies $0M \subseteq N \subseteq 1M$).

2.3. Abelian groups as $\mathbb{Z}$-modules

We shall now try to understand $\mathbb{Z}$-modules in particular.

Let us recall one of the most basic definitions in elementary mathematics: the definition of multiplication of integers.

Multiplication of nonnegative integers was defined by repeated addition: If $n, m \in \mathbb{N}$, then nm means $\underbrace{m + m + \cdots + m}_{n \text{ times}}$. This same formula $nm = \underbrace{m + m + \cdots + m}_{n \text{ times}}$ can be applied to negative integers m as well, but not to negative integers n, since there is no such thing as $\underbrace{m + m + \cdots + m}_{-5 \text{ times}}$. Thus, the product nm for negative n had to be defined differently; one way to define it is by setting $nm = -\left(\underbrace{m + m + \cdots + m}_{-n \text{ times}}\right)$. Thus, for arbitrary integers n and m, the product nm is defined by

$$nm = \begin{cases} \underbrace{m + m + \cdots + m}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{m + m + \cdots + m}_{-n \text{ times}} \right), & \text{if } n < 0. \end{cases}$$

The same definition can be adapted to any abelian group:

Proposition 2.3.1. Let A be an abelian group, written additively (i.e., the operation of A is denoted by $+$, and the neutral element by 0). For any $n \in \mathbb{Z}$ and $a \in A$, define

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}} \right), & \text{if } n < 0. \end{cases} \tag{3}$$

Thus, we have defined a map

$$\begin{aligned} \mathbb{Z} \times A &\to A, \\ (n, a) &\mapsto na. \end{aligned}$$

We shall refer to this map as the **action of $\mathbb{Z}$ by repeated addition** (due to the way na was defined in (3)).

(a) The group A becomes a $\mathbb{Z}$-module, where we take this map as the action of $\mathbb{Z}$ on A.

(b) This is the **only** $\mathbb{Z}$-module structure on A. That is, if A is **any** $\mathbb{Z}$-module, then the action of $\mathbb{Z}$ on A is given by the formula (3) (and therefore is uniquely determined by the abelian group structure on A).

(c) The $\mathbb{Z}$-submodules of A are precisely the subgroups of A.

Proof. See the text (§3.4). □

Proposition 2.3.1 reveals what $\mathbb{Z}$-modules really are: They are just abelian groups with a more convenient "user interface". The "scaling by repeated addition" structure is inherent in the group, and by making the group into a $\mathbb{Z}$-module, you are "exposing" it for easy use.

In contrast, for a typical ring R, the R-modules have much more structure than the underlying abelian groups. In particular, two R-modules can often be isomorphic (or even identical) as abelian groups yet non-isomorphic as R-modules. To put it differently, the action of a ring R on an R-module M is not usually uniquely determined by the addition of M. That it is so determined for $R = \mathbb{Z}$ is an exception.

But $\mathbb{Z}$ is not the only exception! Another case where the R-module structure is uniquely determined by the addition is the case when $R = \mathbb{Q}$. The $\mathbb{Q}$-modules are also known as $\mathbb{Q}$-vector spaces (since $\mathbb{Q}$ is a field), and again the action of $\mathbb{Q}$ on such a $\mathbb{Q}$-module is uniquely determined by its addition: If a is a vector in a $\mathbb{Q}$-module M, and if $q = \dfrac{n}{m}$ is a rational number (where n and m are integers), then qa is the unique $b \in M$ that satisfies $mb = na$ (and the multiples mb and na here can be computed by the formula (3) using repeated addition)[1]. Thus, any abelian group becomes a $\mathbb{Q}$-module in at most one way. However, not every abelian group can be made into a $\mathbb{Q}$-module in the first place! For instance, $\mathbb{Z}/2$ does not become a $\mathbb{Q}$-module, because if it did, then the vector

$$\frac{1}{2} \cdot \left(2 \cdot \overline{1}\right) = \underbrace{\left(\frac{1}{2} \cdot 2\right)}_{=1} \cdot \overline{1} = 1 \cdot \overline{1} = \overline{1}$$

would be equal to

$$\frac{1}{2} \cdot \underbrace{\left(2 \cdot \overline{1}\right)}_{=\overline{2}=\overline{0}} = \frac{1}{2} \cdot \overline{0} = \overline{0},$$

which it is not.

Thus, we see that turning an abelian group into a $\mathbb{Q}$-module is not always possible, but the result is always unique if it exists.

What about $\mathbb{R}$-modules? Again, not every abelian group can be made into an $\mathbb{R}$-module (for instance, $\mathbb{Q}$ is not an $\mathbb{R}$-module). But this time, uniqueness is not a given either: In an $\mathbb{R}$-module, the action of $\mathbb{R}$ is never uniquely determined by the addition, unless the $\mathbb{R}$-module is trivial (i.e., just contains a single vector). Likewise, the action of the ring $\mathbb{Z}[i]$ on a $\mathbb{Z}[i]$-module is usually not uniquely determined by the addition (see, e.g., the two different $\mathbb{Z}[i]$-modules $\mathbb{Z}/5$ we constructed in §2.1.5).

2.4. Module morphisms

2.4.1. Definition

Ring morphisms are maps between rings that respect the defining features of a ring (addition, multiplication, zero and unity).

Module morphisms play a similar role for modules instead of rings. But they are also known under a different name: linear maps. Here is their definition.

Definition 2.4.1. Let R be a ring. Let M and N be two left R-modules.

(a) A **left R-module morphism** (or, for short, a **left R-linear map**) from M to N means a map $f : M \to N$ that

[1] This isn't really obvious, but it is not hard to prove. (This is essentially Winter 2021 Homework set #3 Exercise 3.)

- **respects addition** (i.e., satisfies $f(a+b) = f(a) + f(b)$ for all $a, b \in M$);
- **respects scaling** (i.e., satisfies $f(ra) = rf(a)$ for all $a \in M$ and $r \in R$);
- **respects the zero** (i.e., satisfies $f(0_M) = 0_N$).

You can drop the word "left" and just say "R**-linear map**" or "R**-module morphism**" if there is no confusion to fear.

(b) A **left R-module isomorphism** from M to N means an invertible left R-module morphism $f : M \to N$ whose inverse $f^{-1} : N \to M$ is also a left R-module morphism.

(c) The left R-modules M and N are said to be **isomorphic** if there is a left R-module isomorphism from M to N. In this case, we write "$M \cong N$".

(d) Right R-module morphisms (and isomorphisms) are defined similarly.

2.4.2. Simple examples

Here are some examples of R-module morphisms:

- When F is a field, the F-module morphisms are precisely the F-linear maps you know from linear algebra.
- Let $k \in \mathbb{Z}$. The map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto ka$ is always a $\mathbb{Z}$-module morphism.
- More generally: Let R be a ring. Let k be a **central** element of R. Let M be any left R-module. Then, the map

$$M \to M,$$
$$a \mapsto ka$$

  is a left R-module morphism. (Check this – and make sure you see where the "central" condition is being used!)

- Let R be a ring. Let $n \in \mathbb{N}$. For any $i \in \{1, 2, \ldots, n\}$, the map

$$\pi_i : R^n \to R,$$
$$(a_1, a_2, \ldots, a_n) \mapsto a_i$$

  (which sends each n-tuple to its i-th entry) is a left R-module morphism.

  Similar things hold for direct products of the form $M_1 \times M_2 \times \cdots \times M_n$: Let $M_1, M_2, \ldots, M_n$ be any n left R-modules. Then, for any $i \in \{1, 2, \ldots, n\}$, the map

$$\pi_i : M_1 \times M_2 \times \cdots \times M_n \to M_i,$$
$$(a_1, a_2, \ldots, a_n) \mapsto a_i$$

  is a left R-module morphism.

- If M and N are two left R-modules, then the map

$$M \times N \to N \times M,$$
$$(m, n) \mapsto (n, m)$$

is an R-module isomorphism.

The $\mathbb{Z}$-module morphisms (i.e., the $\mathbb{Z}$-linear maps) are just the group morphisms of the additive groups:

Proposition 2.4.2. Let M and N be two $\mathbb{Z}$-modules. Then, the $\mathbb{Z}$-module morphisms from M to N are precisely the group morphisms from $(M, +, 0)$ to $(N, +, 0)$.

Proof. Easy exercise. □

2.4.3. Ring morphisms as module morphisms

Here is one more source of R-module morphisms:

- Let R and S be two rings. Let $f : R \to S$ be a ring morphism.

  As we discussed in §2.1.5 (Lecture 18), this morphism f makes S into a left R-module by the rule

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

  This action is called the action on S induced by f.

  It is now easy to see that f is a left R-module morphism from R to S. For instance, it respects scaling because

$$f(ra) = rf(a) \qquad \text{for all } r \in R \text{ and } a \in R$$

  (since f is a ring morphism, and thus we have $f(ra) = f(r) \cdot f(a) = rf(a)$ by the definition of the action of R on S).

  Here is a specific example: There is a ring morphism

$$f : \mathbb{C} \to \mathbb{C},$$
$$a + bi \mapsto a - bi \qquad (\text{for all } a, b \in \mathbb{R}).$$

  This morphism f is called **complex conjugation** (and geometrically can be viewed as reflection across the real axis); the image $f(z)$ of a complex number z is commonly denoted by $\overline{z}$.

  Obviously, $\mathbb{C}$ is a $\mathbb{C}$-module, with the action being given by multiplication. However, we can define a second $\mathbb{C}$-module structure on $\mathbb{C}$, which is induced by the morphism f (as explained in §2.1.5). This second structure has the same addition as the first, but its action is given by

$$r \rightharpoonup s = \underbrace{f(r)}_{=\overline{r}} \cdot s = \overline{r} \cdot s \qquad \text{for any } r, s \in \mathbb{C},$$

where $r \rightharpoonup s$ means the result of scaling s by r using this second $\mathbb{C}$-module structure (i.e., the image of (r, s) under the action of $\mathbb{C}$ on this second $\mathbb{C}$-module). (I would normally denote this result by $r \cdot s$, but here I cannot, since $r \cdot s$ already means the usual product of r with s.)

Thus, we have found two ways of scaling a complex number s by a complex number r: The first way yields the usual product $r \cdot s$, while the second way yields $\overline{r} \cdot s$. These two ways provide two $\mathbb{C}$-modules which both are identical to $\mathbb{C}$ as sets and have the same addition, but have different actions. Let me keep denoting the first of them by $\mathbb{C}$, but denote the second by $\overline{\mathbb{C}}$. Then, the map f (i.e., complex conjugation) is not $\mathbb{C}$-linear as a map from $\mathbb{C}$ to $\mathbb{C}$, but it is $\mathbb{C}$-linear as a map from $\mathbb{C}$ to $\overline{\mathbb{C}}$.

More generally, if M is any $\mathbb{C}$-module, then we can define a second $\mathbb{C}$-module structure on M by restricting the $\mathbb{C}$-module M via the complex conjugation map f. This second $\mathbb{C}$-module will be called $\overline{M}$; it agrees with M in its addition, but its action is given by

$$r \rightharpoonup m = \overline{r} \cdot m \qquad \text{for any } r \in \mathbb{C} \text{ and } m \in M,$$

where $r \rightharpoonup m$ means the result of scaling m by r using this second $\mathbb{C}$-module structure, whereas $\overline{r} \cdot m$ means the result of scaling m by $\overline{r}$ using the original $\mathbb{C}$-module structure on M. You can think of $\overline{M}$ as a "mirror image" of the $\mathbb{C}$-module M, which has the same vectors as M but "sees the scalars through a looking glass".

If M and N are two $\mathbb{C}$-modules, then a map $g : M \to N$ is said to be **antilinear** (or **conjugate-linear**) if it is a $\mathbb{C}$-linear map from M to $\overline{N}$. Explicitly, this means that g has the following properties:

$$g(a+b) = g(a) + g(b) \qquad \text{for all } a, b \in M;$$
$$g(ra) = \overline{r} g(a) \qquad \text{for all } r \in \mathbb{C} \text{ and } a \in M;$$
$$g(0) = 0.$$

Thus, in particular, the complex conjugation map f is an antilinear map from $\mathbb{C}$ to $\mathbb{C}$ (or a linear map from $\mathbb{C}$ to $\overline{\mathbb{C}}$).

Antilinear maps appear frequently in complex linear algebra. For example, the standard dot product

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R},$$
$$\left(\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} \right) \mapsto v_1 w_1 + v_2 w_2 + \cdots + v_n w_n$$

is linear in both of its arguments, whereas the Hermitian dot product

$$\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C},$$
$$\left(\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} \right) \mapsto \overline{v_1} w_1 + \overline{v_2} w_2 + \cdots + \overline{v_n} w_n$$

is antilinear in its first argument and linear in its second (which means that it becomes linear in both arguments if we view it as a map from $\overline{\mathbb{C}^n} \times \mathbb{C}^n$ to $\mathbb{C}$). Maps with the latter property are called **sesquilinear**, and in particular all Hermitian forms are sesquilinear.